

NET SECRET'S
N°1 Octobre - novembre 2006 / 3,80 euros
PROTEGEZ TOTALEMENT VOTRE MACHINE
du bios à l'Internet
Rencontres Mondiales du Logiciel Libre
notre reportage aux RMLL 2006
Grand jeu concours :
gagnez une PSP !!!
SONY
Dopez firefox légalement
L 14489 - 1 - F: 3,80 € - RD



Edito

Vous tenez en main le Net Secret's numéro 1. Le Net Hacker's est sorti de l'adolescence et approche de sa maturité en devenant Net Secret's. Vos remarques, sur le chat ou par mail, nous ont permis de le rendre proche du lectorat. Le but premier est toujours présent, c'est à dire, permettre aux « novices », ou newbies, d'apprendre les principes de base du hacking, reversing, programmation ... et aux « avancés » d'asseoir leurs connaissances, de se rafraîchir la mémoire. Au fil des magazines, de nouveaux auteurs ont fait leur apparition ce qui a permis de bousculer un peu la routine. Nous sommes début septembre et c'est la rentrée scolaire. J'ai toujours eu des tas de bonnes résolutions pour la rentrée après un mois de réflexion sous le soleil, les doigts de pied en éventail. La tête fourmille d'idées et j'ai un an pour essayer de les mettre en pratique. D'ailleurs dans ce magazine un jeu concours va vous être proposé avec à la clé une psp à gagner. Le but du concours est de créer le site web de Net Secret's mais en utilisant un cms (content management system en anglais c'est à dire un système de gestion de contenu) qui est en licence GPL du nom de SWIR (site web à implémentation rapide). Mais vous en saurez plus en lisant le dossier. Vous serez peut être surpris de voir d'ici quelques semaines en kiosque, un « grand frère » de Net Secret's, le netsenior qui, comme son nom l'indique, s'adresse à nos sages, les seniors. En effet, l'informatique est maintenant omniprésent dans la plupart des foyers et des besoins diverses se font ressentir. Pour garder la ligne directrice du départ de Net Secret's nous avons préféré créer un nouveau magazine spécifique aux seniors. Vous découvrirez aussi vers le mois de mai la création d'un challenge de sécurité. Mais ne dévoilons pas dés maintenant toutes les surprises de cette année. Nous allons essayer d'être au plus proche de la réalité de la sécurité informatique, de vous aider à forger votre idée sur cette branche de l'informatique , de vous donner toutes les nouvelles fraîches, en somme, faire de la veille technologique. Toute l'équipe de Net Secret's vous souhaite une bonne rentrée et n'oubliez pas notre litemotive : « ce magazine est fait pour vous et évolue grâce à vous ».

FaSm

netsecrets@acissi.net

Sommaire

Les News du net p.4

Trouver des bugs grâce à un GNU ! p.6

Faut savoir ranger ses sockets !! p.9

Scannez comme dans Matrix p.12

Retour sur une épreuve de la Nuit du Hack : PatchMe p.15

La pile perd la mémoire p.17

Paramétrer son routeur correctement p.20

Comment protéger sa machine de l'Internet jusqu'au bios p.24

Grand concours SWIR p.27

Surfez avec TUX p.35

Les scripts bash sous Linux p.38

Firefox, Qu'il est rusé ce renard p.42

Le dictionnaire du hacker p.47

Xbox 360 ou PSP, il y a toujours une faille à exploiter pour profiter à fonds de sa console... p.48

Les 7e Rencontres Mondiales du Logiciel Libre p.52

Courrier des lecteurs p.55

NET SECRET'S
est édité par la Pieuvre noire,
26 bis rue Jeanne d'Arc 94160

Représentant légal : O. André
Principaux associés : O. André et O. Spinelli
Rédacteur en chef : Franck Ebel
Conception Graphique : Weel
ISSN en cours
Numéro de comission paritaire en cours
Dépot légal à parution

Directeur de publication : Olive André

Imprimé en France par Roto garonne
Z.A. "Mestre-Marty" 47310 Estillac

Les News d

Deux failles sévères dans Linux 2.6



Deux vulnérabilités ont été mises sur le devant de la scène durant le week-end.
L'une d'elle, plus ancienne, aurait permis le piratage d'un serveur du projet Debian. Les deux failles frappent la version 2.6 du noyau et sont exploitables localement afin d'obtenir un accès complet au système.
Deux vulnérabilités ont été annoncées pour la version 2.6 du noyau Libre et des exploits sont disponibles sur Internet afin d'en tirer partie.
Un serveur du projet Debian a été compromis via la première de ces vulnérabilités, annoncée le week-end précédent (Linux Kernel "prctl" Privilege Escalation Vulnerability).
Le serveur serait tombé après qu'un pirate soit parvenu à voler l'identité d'un développeur, à se connecter sous le compte aux droits restreints de sa victime puis à prendre le contrôle du système à l'aide d'un tel code publié sur Internet (prctl() suidsafe exploit).
La seconde vulnérabilité a été annoncée et pour elle aussi un code d'exploitation a été publié. Le SANS Institute l'a testé avec succès sur SuSE Linux (noyau 2.6.x) à jour de tous les correctifs. L'organisme précise toutefois que l'extension SELinux bloque l'exploit, et que les machines sous Red Hat Enterprise 4 - qui l'intègre - ne sont donc pas vulnérables.

Microsoft : un été chaud !



Sept bulletins d'alerte, cinq vulnérabilités critiques et un ver potentiel
La première livraison estivale des correctifs de Microsoft est particulièrement riche. Retour sur les failles les plus significatives... et présentation de deux nouvelles !
Parmi les sept bulletins d'alerte publiés par Microsoft pour le mois de juillet, deux axes majeurs sortent du lot : une série de correctifs pour la suite Office, dont certaines failles étaient déjà exploitées durant ces dernières semaines, et une vulnérabilité inédite pour Windows capable de donner naissance à un ver.

Mots de passes trop vieux

Les entreprises françaises font peu de cas du contrôle d'accès
C'est en tout cas ce qui ressort de l'étude "Politiques de sécurité des systèmes d'information et sinistralité en France" rendue publiquepar le Clusif.

A la question "Quelles technologies de contrôle d'accès utilisez vous", les entreprises françaises semblent bien en peine de faire preuve d'originalité.
C'est l'un des enseignements tirés de l'étude "Politiques de sécurité des systèmes d'information et sinistralité en France" publié cette semaine par le Clusif.

Modèles d'habilitation sur la base de profils, workflow d'approbation des habilitations, mots de passe à usage unique, SSO, biométrie, certificats... autant de technologies aux abonnés absents chez les entreprises interrogées.

Aucune des approches suggérées par le Clusif n'est mise en oeuvre de façon majoritaire. Certaines, telles la biométrie, le web SSO ou le provisionning sont mêmes ignorées par près de 90% des entreprises.
Le meilleur score - mais tout est relatif - est obtenu par les certificats numériques, utilisés, expérimentés ou bientôt déployés par 43% du panel interrogé. La TeleTVA ne doit pas y être pour rien. Mais à y regarder de plus près, les entreprises qui utilisent réellement un certificat numérique pour l'authentification ne sont que 10%. Le reste, ce sont des pilotes ou des projets pour l'année en cours.

Le bon vieux mot de passe, et ses incidents de sécurité, a encore de beaux jours devant lui...

du net

web:
http://www.lesnouvelles.net

Mots de passes trop longs



Le problème de sécurité découle de l'utilisation de « passphrases » trop simples qui pourraient être rapidement déchiffrées.
Un outil démontrant l'exploitabilité de cette faille a été mis en ligne le 5 Novembre.

L'équipe à l'origine de cette preuve par l'exemple (proof of concept) est celle qui a également développé « tinyPEAP », un firmware sécurisé pour routeur WiFi Linksys (RADIUS avec 802.1X et PEAP).

Pour utiliser cet outil, il suffit de capturer les données dans un format spécifique (du type de ceux utilisés par les sniffers de type Ethereal) et l'outil applique sur les données son algorithme de craquage. Seules certaines clés courtes ou basées sur des mots usuels sont facilement « déchiffrables »

Un réseau wifi sur trois faillible



La sécurité étant par essence un « process » récurrent, RSA Security sort la quatrième édition de son étude sur la sécurité des WLANs. Alors que l'année dernière 15 pourcent des réseaux testés à Londres étaient vulnérables, cette année le constat est dramatique avec un taux de 36 pourcent de WLANs faillibles.

L'étude a démontré une fois de plus que les protections basiques comme la modification des paramètres de configurations par défaut n'étaient pas respectées. A Londres, ce cas de figure représente 26 pourcent des bornes WiFi testées, ce qui facilite d'autant les attaques potentielles.

Tim Pickard, de RSA, annonce qu' « En matière de WiFi le centre d'affaire de Londres peut être comparé au terrain de jeu d'un voleur qui essayerait d'ouvrir toutes les portes des voitures en espérant être chanceux ». « Nos recherches montrent que des réseaux d'entreprise continuent de croître avec un facteur de 62 pourcent et qu'en même temps 36 pourcent de ces réseaux sont vulnérables ».

Spam : tous complices ?



Le chiffre est significatif : 97% des ordinateurs qui envoient du courrier électronique seraient contrôlés par des spammeurs. Et si l'on y ajoute les serveurs mal configurés et une pincée d'autres problèmes courants, c'est en définitive 99% des ordinateurs qui seraient peu fiables pour envoyer des courriers. L'étude provient de la société Return Path, qui a bien entendu une solution à vendre. Mais les chiffres demeurent intéressants.
Sur les vingt millions d'ordinateurs émetteurs de courrier électronique surveillés par la société Return Path, près de 97% seraient purement et simplement des "usine à spam". Il s'agit, bien entendu, essentiellement de PC familiaux détournés et assemblés en "botnets". Selon Return Path, il serait possible de totalement bloquer ces ordinateurs sans perdre pour autant (trop) de courriers légitimes.

Trouver des bugs

Quoi de plus difficile que de retrouver un bug dans un programme surtout si celui ci n'est pas ou mal commenté ? Beaucoup d'outils sont disponibles sur le web mais peu ont toute la souplesse et les fonctionnalités de GDB.

Introduction

GDB est l'acronyme de Gnu DeBugger. C'est un debugger puissant dont l'interface est totalement en ligne de commande, c'est à dire avec une invite en texte. GDB est tellement apprécié qu'on le trouve aussi encapsulé dans des interfaces graphiques, comme XXGDB ou DDD. GDB est publié sous la licence GNU GPL et gratuit par effet de bord.

Notre programme

Pour pouvoir débugger un programme, il nous en faut un ;-)
Ce n'est pas la peine de prendre compliqué, le but est de comprendre les fonctionnalités de GDB .

```
#include <stdio.h>

int main(){

char input[5];
int i=0;

scanf("%s",input);

for(i=strlen(input);i>=
0;i--)
    {
printf("%c",input[i]);}
printf("\n");

return 0;
}
```

Vous devez, pour debugger ce programme, le compiler avec les options de debuggage, ceci pourra être fait en utilisant l'option -g :

```
gcc monprog.c -g -o
monprog
g++ monprog.cpp -g -o
monprog
```

Choisissez bien sur la ligne correspondante au langage utilisé, C ou C++.
essayez ce programme, il faut entrer une chaîne de caractère et celle-ci est affichée à l'écran, à l'envers.

GDB en détails

maintenant que nous avons compilé notre programme, nous pouvons lancer le debugger.

```
fasm@FaSm:~/nethackers$
gdb ./monprog
GNU gdb 6.4-debian
Copyright 2005 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as
"i486-linux-gnu"...Using host libthread_db library
"/lib/tls/i686/cmov/lib
thread_db.so.1".
(gdb)
```

Vous obtenez maintenant un prompt gdb, vous êtes maintenant dans le debugger. Vous avez la possibilité d'utiliser 8 commandes principales :
break, run, print, next, step, continue, display et where

essayons de comprendre ces 8 commandes.

La commande break :

Si vous souhaitez faire une pause à une ligne spéciale de votre programme, par exemple à la ligne 6 (int i=0).

```
(gdb) break 6
Breakpoint 1 at
0x80483b5: file mon-
prog.c, line 6.
(gdb)
```

Il suffit donc de dire à gdb break 6 ce qui aura pour effet d'arrêter le programme à cette ligne lors de l'exécution.

La commande run :

Comme vous vous en doutez, cette commande va permettre de lancer le programme. Celui ci va être normalement lancé (comme si vous etiez en dehors de gdb) et ce jusqu'à ce qu 'il rencontre un breakpoint (ligne 6 pour nous).

```
(gdb) run
Starting program:
/home/fasm/nethackers/m
onprog
```

grâce à un GNU !

```
Breakpoint 1, main ()
at monprog.c:6
6        int i=0;
(gdb)
```

Vous pouvez remarquer que le programme est arrêté et que la ligne en face du breakpoint est rappelée.

Si vous utilisez run de nouveau, gdb vous demande si vous voulez relancer le programme du début ou non.

```
(gdb) run
The program being
debugged has been star-
ted already.
Start it from the
beginning? (y or n) n
Program not restarted.
(gdb)
```

La commande print :
La commande print va vous permettre de voir les valeurs prises par les différentes variables de votre programme. cette commande demande un argument qui est le nom de la variable voulue.

```
(gdb) print i
$1 = 0
(gdb)
```

Nous voyons ici que la variable i à pour valeur 0.

La commande Next and Step :
Ces deux commandes font en gros, la même chose, c'est à dire passer à l'instruction suivante. La seule différence est que la commande next va permettre d'entrer dans une fonction tandis que step va passer par « dessus » de la fonction.

```
(gdb) step
8
scanf("%s",input);
(gdb) print i
$2 = 0
(gdb) next
test
10
for(i=strlen(input);i>=
0;i--)
(gdb)
```

Que s'est il passé ? step a permis de passer à l'instruction suivante, le scanf. Si maintenant je redemande de donner la valeur de i (print i), on voit que i vaut toujours 0.
Si ensuite je demande next, on se retrouve avec le curseur clignotant en attente car en effet, nous avons demandé l'instruction suivante, le scanf a donc été exécuté et le programme attend que nous entrions une chaîne de caractère, ce que j'ai fait en entrant test.

La commande continue :

La commande continue permet de continuer le programme après le breakpoint , ce que nous pouvons faire maintenant.

(gdb) continue
Continuing.
tset

Program exited normally.
(gdb)

vous pouvez donc remarquer que le programme se termine normalement et vous pouvez voir le mot tset apparaître qui est bien le mot test à l'envers.

La commande Display :
la commande display va permettre de voir le contenu d'une variable à chaque étape du programme. retirons d'abors notre breakpoint, ajoutons en un à la ligne 11 (devant { printf("%c",input[i]);}) et regardons ce qui se passe.

```
(gdb) del break 1
(gdb) break 11
Breakpoint 2 at
0x80483f1: file mon-
prog.c, line 11.
(gdb) run
Starting program:
/home/fasm/nethackers/n
ethackers_5/nh5_art1/mo
nprog
test

Breakpoint 2, main ()
at monprog.c:11
11        {
printf("%c",input[i]);}
(gdb) display input[i]
1: input[i] = 0 '\0'
(gdb) next
10
for(i=strlen(input);i>=
0;i--)
1: input[i] = 0 '\0'
(gdb) next

Breakpoint 2, main ()
at monprog.c:11
11        {
printf("%c",input[i]);}
1: input[i] = 116 't'
(gdb) next
10
for(i=strlen(input);i>=
0;i--)
1: input[i] = 116 't'
(gdb) next
```

```
Breakpoint 2, main ()
at monprog.c:11
11        {
printf("%c",input[i]);}
1: input[i] = 115 's'
(gdb) next
10
for(i=strlen(input);i>=
0;i--)
1: input[i] = 115 's'
(gdb) next
```

Breakpoint 2, main () at monprog.c:11
11 { printf("%c",input[i]);}
1: input[i] = 101 'e'
...

Vous pouvez voir apparaître chaque lettres de votre mot entré (test) se retrouve dans input[i].

La commande Where :

Cette commande va nous permettre de retrouver l'endroit ou un programme va planter. Lancez le programme et comme chaîne de caractère, entrez





20 « A » par exemple.

```
(gdb) run
Starting program:
/home/fasm/nethackers/
nethackers_5/nh5_art1/
monprog
AAAAAAAAAAAAAAAAAAAA

Program received signal
SIGSEGV, Segmentation
fault.
0x41414141 in ?? ()
(gdb)
```

Vous voyez que le programme s'arrête en vous indiquant que le programme s'est planté.
tapez maintenant where :

```
(gdb) where
#0  0x00414141 in ?? ()
#1  0x00000001 in ?? ()
#2  0xbff75124 in ?? ()
#3  0xbff7512c in ?? ()
#4  0xb7f6bbf6 in
_dl_rtld_di_serinfo ()
from /lib/ld-linux.so.2
Previous frame inner to
this frame (corrupt
stack?)
(gdb)
```

Vous pouvez utiliser la commande up pour remonter dans la pile:

```
(gdb) up
#1  0x00000001 in ?? ()
(gdb) up
#2  0xbff75124 in ?? ()
(gdb) up
#3  0xbff7512c in ?? ()
(gdb) up
#4  0xb7f6bbf6 in
_dl_rtld_di_serinfo ()
from /lib/ld-linux.so.2
(gdb) up
Initial frame selected;
you cannot go up.
```

On quitte donc le programme gdb en marquant quit

CONCLUSION

Vous avez maintenant les bases pour commencer à utiliser gdb. Nous verrons dans d'autres articles comment utiliser gdb pour les buffer overflow (les connaisseurs ont déjà remarqué les prémices d'un bof dans cet article ;-)).
je vous recommande ce site si vous voulez connaître toutes les subtilités de gdb :

http://www.delorie.com/gnu/docs/gdb/gdb_toc.html#SEC_Contents

alors, bon debbugages ...

Faut savoir ranger ses sockets !!

Depuis quelques années les réseaux se développent à vitesse grand V. Ils offrent de nombreuses possibilités dans le domaine de la communication. Ainsi des applications client-serveur comme des logiciels de peer-to-peer ou de chat voient régulièrement le jour. La programmation réseau en C se fait en utilisant ce qu'on appelle des sockets.

Introduction

Les sockets font partie de la couche logiciel de la plupart des systèmes d'exploitation. Les sockets s'utilisent avec les protocoles de la couche 4 du modèle OSI : TCP/IP et UDP/IP mais on utilise plus généralement TCP/IP. Le modèle OSI est un standard reconnu par l'organisation internationale de normalisation (ISO).

Qu'est-ce qu'une socket ?

Une socket est un moyen de communication permettant à une application de communiquer avec d'autres applications. Chacune des applications utilisant les sockets sont identifiées par une adresse IP.
Il existe trois types de communications avec les sockets :

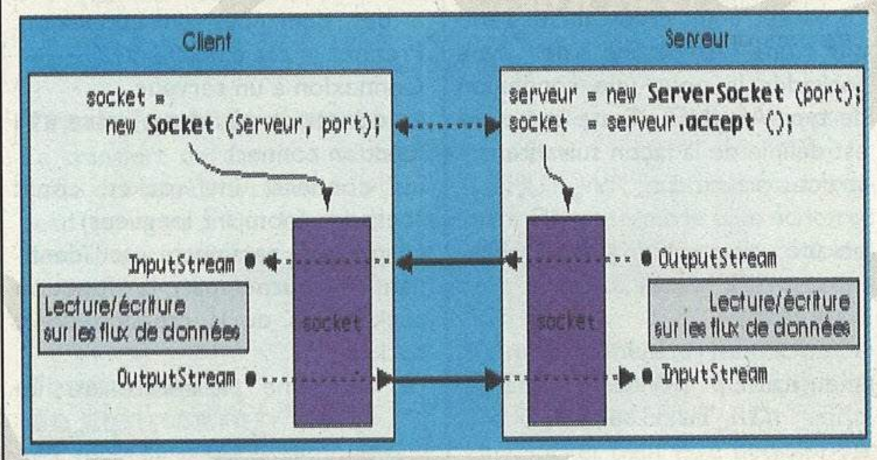
- Les sockets en mode datagramme
- Les sockets en mode connecté
- Les sockets en mode brut

- les sockets en mode datagramme

Il s'agit d'une communication non orientée connexion, c'est-à-dire qu'une application envoie des données à une autre application sans qu'une connexion ai explicitement été établie. Le bon acheminement des données n'est pas garanti, elles peuvent être dupliquées et peuvent arriver dans le désordre ou ne pas arriver du tout.

- les sockets en mode connecté

Contrairement aux sockets en mode datagramme il s'agit d'une communication orientée connexion.
Une socket fait une demande de connexion à une autre socket et celle-ci peut accepter ou refuser la



connexion. Le bon acheminement des données est gara
nti ainsi que leur non duplication et l'ordre de leur envoi.

- les sockets en mode brut (raw en anglais)

Ce mode est semblable au mode connecté, la différence est qu'ici on a la possibilité de remplir soi même les champs de l'entête des paquets de données selon le protocole choisi.

Création d'une socket

Une socket se crée grâce à l'appel système du même nom :

```
int socket ( int domaine, int type,
int protocole )
```

Tous ces paramètres sont des constantes. La fonction socket retourne une valeur de -1 en cas d'erreur et un entier identifiant de socket lorsqu'il n'y a pas d'erreur.
Le premier paramètre désigne le domaine où aura lieu la communication. On utilise AF_INET pour les communications internet mais il existe d'autres valeurs : AF_UNIX pour les communications locales sur les systèmes Unix. AF_INET et AF_UNIX sont les plus utilisés.
Le deuxième paramètre est le type de socket:

- SOCK_STREAM pour le mode connecté

Pour connaître les messages d'erreur de chaque fonction vous pouvez utiliser le man car dans cet article ils n'ont pas tous été repris.

- SOCK_DGRAM pour le mode datagramme
- SOCK_RAW pour le mode brut.

Le dernier paramètre est le protocole que va utiliser la socket. On utilise IPPROTO_TCP pour les communications internet. La valeur zéro met automatiquement ce paramètre au protocole par défaut selon le type de socket choisi, par exemple IPPROTO_UDP pour SOCK_DGRAM ou encore si l'on veut traiter des paquets de type ICMP on utilisera IPPROTO_ICMP.

La structure sockaddr_in

La socket étant créée, il faut remplir une structure de type sockaddr_in pour une connexion de type AF_INET. Cette structure est définie de la façon suivante :

```
struct sockaddr_in
{
short sin_family;
unsigned short
sin_port;
struct in_addr
sin_addr;
char sin_zero[8];
}
```

Le champ sin_family désigne le domaine de la socket et prend la même valeur que celui utilisé par la socket préalablement créée.

Le champ sin_port est le numéro port qui sera utilisé pour la communication. Il se remplit en convertissant le numéro du port grâce à la fonction htons() .

Le champ sin_addr contient une structure de type in_addr dont on utilisera que le champ s_addr car il s'agit d'une union : une structure déclarée avec plusieurs champs qui occupent le même espace en mémoire. Le champ s_addr se remplit avec l'adresse IP des sockets qui pourront se connecter. On utilise généralement la fonction inet_addr pour convertir une adresse ip au format tableau de caractère en adresse ip valide pour remplir ce champ. Un serveur utilisera la constante INADDR_ANY pour accepter toutes les requêtes de connexion.

Le champ sin_zero ne sera pas utilisé. Il équilibre cette structure pour qu'elle ait la même taille en octet que la structure sockaddr ceci afin de permettre les conversions entre ces deux types de structures.

L'étape suivante dépend du type d'application que l'on veut coder, client ou serveur. Une application cliente va se connecter à un serveur alors qu'une application serveur va écouter sur le port définit dans la structure sockaddr_in si il y a des demandes de connexion. Prenons le cas d'un client.

Connexion à un serveur

La connexion s'effectue grâce à la fonction connect :

int connect(int socket, const sockaddr *nom, int longueur)

Le premier paramètre est l'identifiant retourné par la fonction socket lors de la création de la socket.

Le deuxième paramètre est un pointeur sur la structure sockaddr_in remplie plus haut. On convertit la structure sockaddr_in en sockaddr en utilisant un pointeur de type sockaddr et en faisant précéder la structure sockaddr_in d'une esperluette (~).

Le dernier paramètre est la taille de la structure sockaddr_in en octet, on utilise la fonction sizeof.

La fonction connect renvoie un identifiant de socket (int) si la connexion a réussie et la valeur -1 si elle a échouée. L'identifiant de socket renvoyé sera utilisé lors de l'échange de données.

Prenons maintenant le cas du serveur. Il va écouter les requêtes de connexion sur un port pour cela il faut lier la socket à un port d'écoute. Ceci s'effectue à l'aide de



la fonction bind.

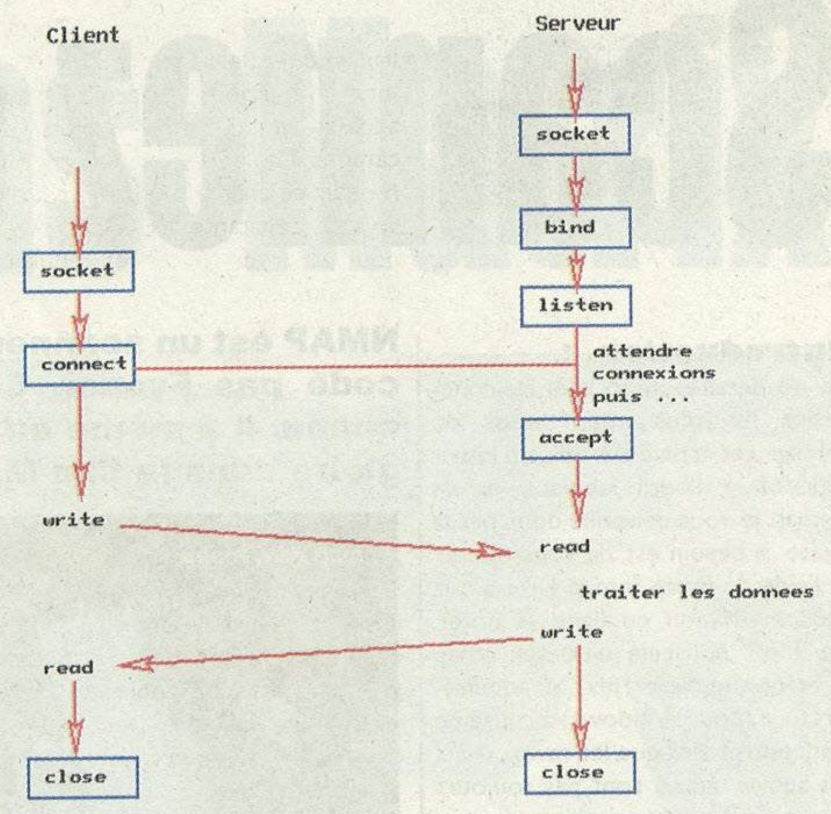
int bind(int socket, const sockaddr *nom, int longueur)
Les paramètres de la fonction bind sont les mêmes que ceux de la fonction connect. La fonction bind renvoie 0 si il n'y a pas d'erreur et -1 en cas d'erreur.

Mise sur écoute

On utilise la fonction listen :
int listen(int socket, int backlog)
Le premier paramètre est la valeur retournée par la fonction socket.
Le deuxième paramètre est le nombre maximal de demande de connexion que pourra traiter le serveur.
La valeur de retour est 0 si il n'y pas d'erreur et -1 en cas d'erreur.
Après la mise en écoute du serveur, celui-ci doit pouvoir accepter des connexions, ceci avec la fonction accept.

Accepter une connexion

int accept(int socket, struct sockaddr * nom, int longueur)
Le premier paramètre est l'identifiant de la socket créée.
Le deuxième paramètre est un pointeur sur une structure de type sockaddr_in. Lors de la connexion cette structure sera remplie avec les informations sur l'application cliente : le port utilisé et l'adresse IP. Ce paramètre doit être NULL si nous n'avons pas besoin de ces informations.
Le troisième paramètre est la longueur en octet de la structure passée en deuxième paramètre si on a utilisé une structure. Ce paramètre doit être NULL si nous n'avons pas utilisé de structure.
La fonction accept attend les demandes de connexions avant de renvoyer un autre identifiant de socket si il n'y pas eu d'erreur et la constante INVALID_socket dans le cas contraire. Le nouvel identifiant de socket renvoyé sera utilisé lors des fonctions d'échange de données.



déroulement classique d'une application de type client serveur

Transfert de données

Le transfert de données se fait à l'aide des appels système habituels read et write à qui l'on passe le descripteur de fichier d'une socket connectée comme premier paramètre.

Fermeture de connexion et destruction

Les deux sens de la connexion peuvent être fermés à l'aide de l'appel système
int shutdown(int s, int how);
Le paramètre s est le descripteur de fichier de la socket ; le paramètre how indique le sens à fermer, il peut être :
– SHUT_WR, qui envoie un segment FIN et ferme le coté écriture ;
– SHUT_RD, qui ferme le coté lecture et cause l'envoi de segments RST si
d'autres données arrivent ;
– SHUT_RDWR, qui combine SHUT_WR et SHUT_RD.
Une socket peut être détruite par un appel à close.

> L'adresse du pair distant est normalement connue aussi bien par le client (qui
> sait à quelle adresse il s'est connecté) que par le serveur (qui l'a obtenue lors de l'appel à accept). On peut l'obtenir de nouveau à l'aide de l'appel système int getpeername(int s, struct sockaddr *name, socklen_t *namelen);

CONCLUSION

Vous connaissez maintenant les principes de base pour commencer à utiliser les sockets en C afin de faire dialoguer deux ordinateurs entre eux. N'hésitez pas à relire l'article sur ethereal du NetHackers3 et de vous en servir pour voir le déroulement de la discussion entre les deux pc lors de l'exécution de votre programme en C.

LuCiF3R

Scannez comm

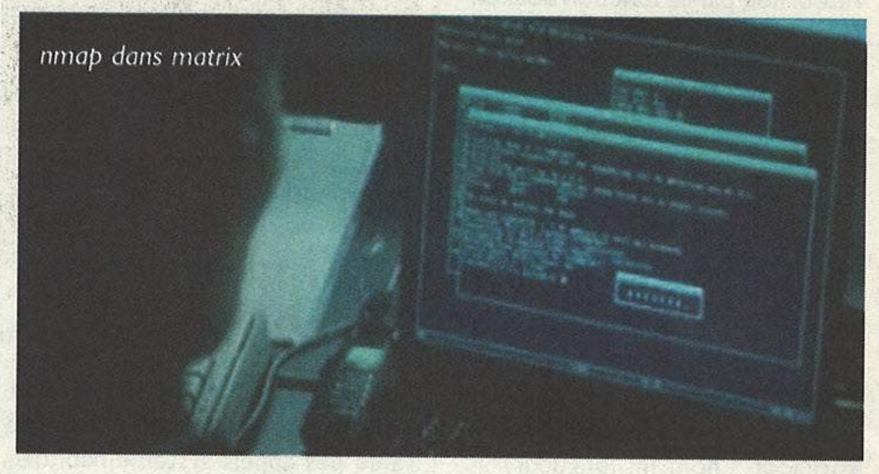
Introduction :

Je ne détaillerais ici que les fonctions les plus importantes de Nmap ,cet article fait office d'introduction à l'outil fabuleux qu'est Nmap, je vous conseille donc par la suite ,si besoin est, de vous referer à l'aide de nmap (nmap –h) ou à la documentation en ligne. A noter, qu'il est conseillé d'utiliser nmap en tant que root (*nix) ou administrateur (pour Windows) à cause de fonctions telles que les raw sockets et autres qui ne sont pas toujours permises en tant qu'utilisateur normal. Et pour finir cette introduction, si vous ne vous y connaissez pas trop en matière de réseaux internet (TCP-IP,..) n'hésitez pas, dés que vous ne comprenez pas un terme à aller voir l'ami Google.

Les types de scans :

Ca y est vous avez téléchargé nmap sur http://www.insecure.org/ et vous l'avez installé c'est parfait, passons à présent aux choses sérieuses. Quand un utilisateur normal souhaite faire un scan basique il utilise par défaut la commande –sT, cette commande envoie tout simplement une demande de connexion sur chaque port, si la connexion est acceptée alors le port est ouvert. Bien évidemment ce genre de scan est facilement détectable. Un utilisateur root bénéficie, lui par défaut, de la commande –Ss (TCP Syn Scan) , celle-ci est un peu plus élaborée que la commande –sT. Cette commande permet d'envoyer un paquet SYN au serveur sur le(s) port(s) cible(s), si la réponse du serveur est un paquet SYN ou ACK alors, c'est bon le port est ouvert, et nmap clôture la connexion avec un paquet RST.

NMAP est un scanneur très puissant, il a été codé pas Fyodor. Ce programme est très connu, il a même eu droit à son moment de gloire dans le film Matrix ;).


nmap dans matrix

Selon le standard un port fermé renvoie un paquet RST, la commande –sF se base sur ce principe et envoie un paquet FIN pour voir la réaction du serveur. Bien évidemment pour que cela fonctionne il faut que le serveur cible soit conforme au standard, ce type de scan ne marche pas alors sur des systèmes comme Windows, BSDI, Cisco, IRIX, MVS, …

Nmap intègre aussi la fonction ping avec la commande –sP, de plus en plus de serveurs bloquent aujourd'hui le ping, il faut alors utiliser la commande –P0 pour scanner les IPs qui ne répondent pas aux pings (donc qui refuse les requetes/réponses ICMP).

Toutes les techniques de scan présentées ci-dessus utilisent les ports TCP. Pour scanner des ports UDP, il faut faire appel à la commande –sU qui peut parfois être bien longue à cause des restrictions sur certains OS (excepté Windows).

Note : -v est une option bien utile elle vous donne plus de détails sur le scan en cours, vous pouvez même faire un –vv pour encore plus détails. Un scan ordinaire avec la commande : nmap -sS -P0 1.2.3.4 donnerait comme résultat :

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2006-07-31 19:49 Paris, Madrid
Interesting ports on 1.2.3.4:
Not shown: 1669 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
110/tcp  open     pop3
```

ne dans Matrix

```
111/tcp open     rpcbind
113/tcp open      auth
135/tcp filtered msrpc
143/tcp open      imap
445/tcp filtered micro-
soft-ds
776/tcp open      wpages
```

Nmap finished: 1 IP address (1 host up) scanned in 21.078 seconds

Regardez à présent le résultat avec l' utilisation du mode verbose (en –vv) :

C:\nmap>nmap -sS -v -P0 1.2.3.4

```
Starting Nmap 4.11 (
http://www.insecure.org
/nmap ) at 2006-07-31
19:28 Paris, Madrid
DNS resolution of 1 IPs
took 6.61s.
Initiating SYN Stealth
Scan against 1.2.3.4
[1680 ports] at 19:29
Discovered open port
22/tcp on 1.2.3.4
Discovered open port
21/tcp on 1.2.3.4
Discovered open port
113/tcp on 1.2.3.4
Discovered open port
80/tcp on 1.2.3.4
Discovered open port
25/tcp on 1.2.3.4
Discovered open port
143/tcp on 1.2.3.4
Discovered open port
111/tcp on 1.2.3.4
Discovered open port
110/tcp on 1.2.3.4
Discovered open port
776/tcp on 1.2.3.4
```



```
The SYN Stealth Scan
took 11.50s to scan
1680 total ports.
Host 1.2.3.4 appears to
be up ... good.
Interesting ports on
1.2.3.4:
Not shown: 1669 closed
ports
PORT     STATE      SER-
VICE
21/tcp   open       ftp
22/tcp   open       ssh
25/tcp   open       smtp
80/tcp   open       http
110/tcp  open       pop3
111/tcp  open
rpcbind
113/tcp  open       auth
135/tcp  filtered msrpc
143/tcp  open       imap
445/tcp  filtered micro-
soft-ds
776/tcp  open       wpages

Nmap finished: 1 IP
address (1 host up)
scanned in 18.343
seconds
                  Raw
packets sent: 1759
(77.396KB) | Rcvd: 1755
(70.268KB)
```

Nmap est riche en options :

Pour les paranos (et oui il y en a !!) nmap a une commande permettant de prendre en argument une adresse IP afin de scanner une machine. C'est-à-dire par exemple, que l'on pourra scanner le serveur cible (ServA) en faisant croire à celui-ci que c'est SerB qui le scanne (ServB est l'adresse IP passée en argument) alors que c'est bel est bien vous qui à l'origine scannez… Cela est possible grâce à l'option –sI. Si vous souhaitez juste scanner une plage de port ou un port seul, il faut utiliser l'option –p. Celle-ci prend en argument donc un port (ex : 666) ou une plage de port (ex : 0-358). Un scan sans l'option –p scannera par défaut les ports de 1 a 1024. Cette option –p permet aussi de choisir de scanner les ports UDP ou TCP on peut donc faire une commande dans le genre :

```
nmap -sU -P0 -p
U:14,120,T:21,80
127.0.0.1

-sU : pour signaler
qu'on va scanner du
UDP.
 -p : l'option magique
décrite ci-dessus ?
U : On met « U » devant
un numéro de port UDP
T : Et « T3 devant un
numéro de port TCP
-P0 : Si l'host bloque
les pings.
Donc ici on signale à
Nmap qu'on va scanner
les ports UDP 14 et
120, ainsi que les
ports TCP 21 et 80 de
l'ip 127.0.0.1.
```

```
C:\nmap>nmap -sU -P0 -p U:14,120,T:21,80 rockweb.org

Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2006-07-31 19:17 Paris, M
adrid
Interesting ports on 195.140.140.196:
PORT     STATE  SERVICE
14/udp   closed unknown
120/udp  closed cfdptkt

Nmap finished: 1 IP address (1 host up) scanned in 7.250 seconds

C:\nmap>
```

résultat nmap -sU –P0 -p U:14,120,T:21,80 127.0.0.1

Voilà un exemple de résultat :

nmap -sU -p 18-21,5000- 127.0.0.1
Cette commande demandera à nmap de scanner la plage de ports TCP compris 18 et 21 et les ports supérieurs à 5000 de l'IP 127.0.0.1.
Si vous désirez spécifier un port source pour votre scan, utilisez l'option –g suivit du numéro de port. Cette option est utile pour tromper certaines protections.

Nmap permet aussi de spécifier la vitesse du scan grâce à l'option –T suivit du mode (ici du plus lent au plus rapide) : Paranoid, Sneaky, Polite, Normal, Agressive, Insane (Normal est le mode par défaut). Pour le mode Paranoid il faut compter cinq minutes entre chaque paquet envoyé !

Pour conclure cet article, je vais vous montrer comment on peut scanner une plage d'IP grâce à NMAP. Si vous souhaitez scanner une plage d'IP sur un port spécifique ou non c'est simple, reprenons l'exemple présenté plus haut avec l'IP modifiée :

```
nmap -sU -p 18-21,5000-
195.124.0.0
```

Si vous souhaitez effectuer ce type de scan sur une plage d'adresse IP il suffit de faire cela :

```
nmap -sU -p 18-21,5000-
195.124.*.*
```

Nmap scannera donc les machines ayant une adresse IP commençant par « 195.124 ». Une fois arrivé a 195.125.0.0 il s'arrêtera.

Conclusion :

Voilà c'est fini, Nmap possède encore bien d'autres options, mais je ne peux tout expliquer ici, alors n'hésitez pas à faire un nmap –h ou à faire un tour sur le site officiel http://insecure.org/nmap/ ;
Nmap est extrêmement riche en possibilités !!! A un prochain tut ;).

wOrp

Nmap par la fenêtre ?

Des développeurs ont pensés à coder un frontend (une interface gui) pour nmap rendant ainsi l'utilisation de nmap plus facile. Donc, si votre seul peur était de manier les commandes de nmap dans une console vous n'avez plus d'excuses. Sous Windows le frontend le plus connu est NmapWin (http://nmapwin.sourceforge.net).

Retour sur une épreuve de la Nuit du Hack : PatchMe

INTRODUCTION

Cette épreuve avait spécialement été conçue pour illustrer l'utilité de la retro-ingénierie. En effet, cette spécialité, n'en déplaise pour certains, ne sert pas qu'à déplomber des logiciels. Elle rend de nombreux services dans l'industrie du logiciel comme l'ajout de fonctionnalités, l'inter-opérabilité ou la correction de failles et de défauts. C'est précisément à ce tout dernier cas que les participants ont été confronté.

Il est de plus en plus courant de rencontrer des bugs dans un programme et le support des développeurs n'est pas toujours assuré .Si le code source est disponible, le développement d'un correctif reste assez simple. Voyons comment procéder dans le cas où nous ne disposons que du binaire...

```
snake@[redacted] ~/Bureau/Challenges/patchme $ ./patchme 1 5 5 7 36 0
|36|1|5|5|7|0|
snake@[redacted] ~/Bureau/Challenges/patchme $ ./patchme 10 9 8 7 6 5 4 3 2 1 0
|135121|10|9|8|7|6|5|4|3|2|1|
*** glibc detected *** free(): invalid next size (fast): 0x0804a008 ***
Abandon
snake@[redacted] ~/Bureau/Challenges/patchme $
```

Pas très utile ce programme de tri ne triant pas...

ENTRONS DANS LE VIF DU SUJET

Commencez par récupérer l'épreuve sur notre site : http://acissi.net/Net Secrets , puis placez vous dans les conditions réelles. Démarrez sur un système GNU / Linux et décomprimez l'archive. Vous obtiendrez alors trois fichiers : "patchme", "tritab.h" et "tritab.so". Déplacez ensuite ce dernier fichier dans "/usr/lib" et oubliez-le pour le moment car, en tant que participant, vous n'êtes pas sensé connaître sa présence au départ ;-)

"patchme" est un binaire et vous constatez qu'il affiche le tri, dans l' ordre croissant, d'une liste de nombres passée en argument. Vous remarquerez aussi que le tri est toujours invalide et que le programme plante avec certaines suites de nombres comme "10 9 8 ... 1 0".

Regardez maintenant le fichier d'extension ".h". C'est un fichier entête en langage C/C++ qui déclare le prototype d'une fonction : void tritab(int *tableau,int longueur); Cette dernière prend en paramètres un tableau d'entiers et la longueur de celui-ci. D'après son nom, elle doit donc se charger du tri effectué par notre programme.

Il est courant de trouver un fichier entête accompagnant une bibliothèque dont on ne dispose pas le code source afin de pouvoir l'utiliser. Trouvons-la grâce à l'outil ldd qui affiche les bibliothèques nécessaires au bon fonctionnement d'un binaire dont le chemin est passé en paramètres : ldd ./patcheme
Vous constatez alors qu'un fichier du même nom que l'entête, mais avec l'extension ".so", est requis : "tritab.so". Il s'agit d'une bibliothèque à liaison dynamique : un programme qui ne peut pas être directement exécuté, mais qui offre ses services, répartis en fonctions, à d'autres programmes en exécution.

Les bibliothèques ont de nombreux avantages comme la réduction de la taille des binaires, en externalisant une partie du code, et la réutilisation, puisque le code est déjà prêt et testé. Elles rendent également plus simple la maintenance et permettent de décomposer un problème en plusieurs problèmes plus petits => diviser pour mieux régner ! Sous Microsoft Windows, ce sont les fameuses DLL (Dynamic Link Libraries) et donc sous GNU / Linux, les SO (Shared Objects).

Analysons avec le débuggeur GDB l'exécution du programme. Lancez GDB sur ce dernier : gdb ./patchme, puis désassemblez la section "main" : disassemble main et repérez l'appel à la fonction tritab : call 0x8048798 <_Z6tritabPii@plt>. Pour atteindre cette fonction, lancez le programme sans paramètres avec run, pour la réferencer.

Posez alors un point d'arrêt sur l'adresse de la fonction : break _Z6tritabPii et lancez le programme avec une suite de nombres : run 10

```
snake@[redacted] ~/Bureau/challenges/patchme $ gcc -c tritab.cpp
snake@[redacted] ~/Bureau/challenges/patchme $ gcc -o tritab.so -shared tritab.o
snake@[redacted] ~/Bureau/challenges/patchme $ ./patchme 10 9 8 7 6 5 4 3 2 1
|1|2|3|4|5|6|7|8|9|10|
snake@[redacted] ~/Bureau/challenges/patchme $
```

Il faut alors mettre les mains dans le cambouis avec GDB...

9 8 7. Vous constatez que le points d'arrêt est atteint sans problème. Cela met hors de cause le code avant l'appel à la fonction. Désassemblez la fonction : disassemble _Z6tritabPii, localisez l'adresse de la dernière instruction avant que la sortie ne s'effectue : 0xb7f568c4 <_Z6tritabPii+158>: jmp 0xb7f5682e <_Z6tritabPii+8> et posez un point d'arrêt sur cette dernière : break *0xb7f568c4. Remarquez bien le caractère * pour informer GDB qu'il s'agit d'une adresse et que ce saut redirige l'exécution en tout début de fonction, où une comparaison est effectuée. Continuez alors l'exécution : continue. Le point d'arrêt est atteint ! Relancez. Il est encore atteint Après quelques expérimentations, vous constaterez qu'il est atteint n+1 fois où n est le cardinal de l'ensemble des nombres passés en paramètres.

Il s'agirait donc d'un problème de débordement lors du parcours du tableau. La fonction tritab corrompt alors la mémoire, ce qui fait planter ensuite le programme. Cette hypothèse nous amène alors à la réécriture d'une fonction de tri qui satisfait l'entête contenu dans tritab.h (cf encadré). Ok mais comment le programme va-t-il utiliser notre version ? Très simple ! Sous GNU / Linux, vous pouvez surcharger n'importe quelle bibliothèque avec la vôtre via la variable LD_PRELOAD.

Commencez par compiler le code : gcc -c tritab.c, puis créez une bibliothèque dynamique à partir du code objet généré : gcc -o tritab.so -shared tritab.o. Renseignez ensuite LD_PRELOAD avec votre bibliothèque : export LD_PRELOAD=./tritab.so et lancez le programme.

```
0x08048b1c <main+298>:  call   0x8048768 <_ZStlsISt11char_traitsI
reamIcT_ES5_PKc@plt>
0x08048b21 <main+303>:  movl   $0x80487f8,0x4(%esp)
0x08048b29 <main+311>:  mov    %eax,(%esp)
0x08048b2c <main+314>:  call   0x8048788 <_ZNSolsEPFRSoS_E@plt>
0x08048b31 <main+319>:  mov    0xfffffffc(%ebp),%eax
0x08048b34 <main+322>:  mov    %eax,(%esp)
0x08048b37 <main+325>:  call   0x8048818 <_ZdlPv@plt>
0x08048b3c <main+330>:  mov    $0x0,%eax
0x08048b41 <main+335>:  leave
0x08048b42 <main+336>:  ret
0x08048b43 <main+337>:  nop
End of assembler dump.
gdb> break _Z6tritabPii
Breakpoint 1 at 0xb7f2e4bd
gdb> run 10 9 8
Error in re-setting breakpoint 1:
Function "_Z6tritabPii" not defined.
Breakpoint 1 at 0xb7fd54bd
Error while running hook_stop:
Invalid type combination in ordering comparison.
```

C'est déjà mieux après une petite séance de débuggage...

Vous constatez alors que le bug a disparu. La correction ainsi créée est assez simple à appliquer et à distribuer.

CONCLUSION

Si la fonction était directement intégrée, cela aurait été beaucoup moins facile. Pensez donc aux bibliothèques quand vous développez. Sachez qu'il en existe énormément, dans de nombreux langages et pour tout type de projet. Profitez-en ! Et n'hésitez pas à créer les vôtres et les partager...

SnAkE

```
void tritab(int *tableau,int longueur)
{
int maxi, i, temp;

while(longueur>0)
      {
      //recherche de la plus grande valeur du
tableau pas encore triée
      maxi=0;

      for(i=0;i<longueur;i++)
      {
      if(tableau[i]>tableau[maxi]) maxi=i;
      }

      //on échange le plus grand élément avec
le dernier
      temp=tableau[maxi];
      tableau[maxi]=tableau[longueur-1];
      tableau[longueur-1]=temp;

      //on traite le reste du tableau
      longueur--;
      }
}
```

Code source en C d'une nouvelle fonction de tri...

La pile perd la mémoire

Pour pouvoir aborder des articles sur les attaques de types buffer overflow , transmettre des paramètres en assembleur ou tout simplement comprendre le mécanisme des sous programmes, Il devient nécessaire de comprendre le fonctionnement de la pile et de la mémoire.

INTRODUCTION

La pile se situe dans les adresse hautes de la mémoire et est la zone mémoire la plus utilisée dans un programme. La pile sert au programme a empiler des données (ex: variables temporaires d'un sous programme) ou les adresses de retour d'une fonction. Elle est donc très utilisée, essayons donc de comprendre son fonctionnement et son utilisation.

La pile en détails

La pile est un espace mémoire utilisé pour stocker temporairement des valeurs. Lorsqu'on utilise la pile, nous empilons les données des adresse basses vers les adresses hautes , comme si nous empilions des assiettes. Vous reprenez donc les assiettes par le haut, la dernière posée est la première reprise. C'est le principe de la LIFO (last in first out : dernière entrée première sortie).La hauteur de la pile est la valeur du registre BP (ou EBP sur les processeurs 32 bits).

Mais comment accéder à la pile ? Les deux instructions phares sont push et pop.

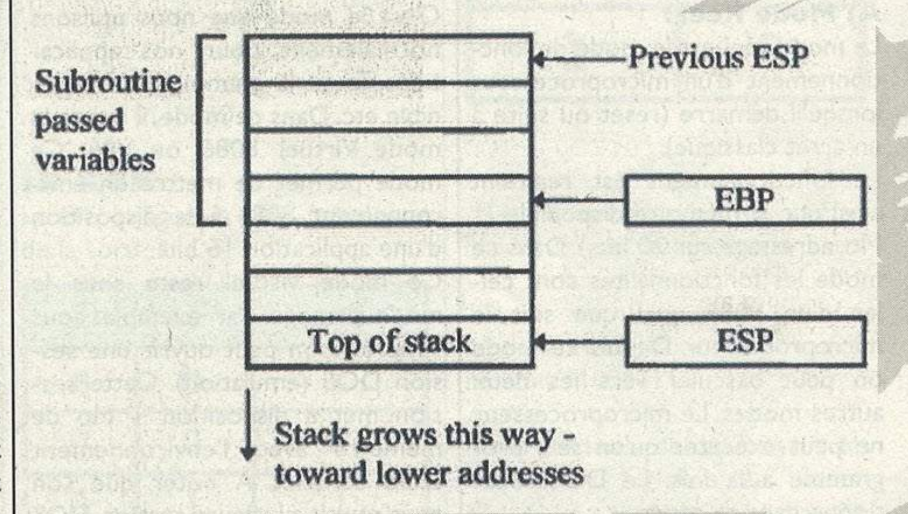
Ces deux instructions prennent un argument qui est soit un registre, soit un nombre.

PUSH permet de faire un transfert vers la pile tandis que POP permet de récupérer ce qui est dans la pile.

```
push eax
push ebx
push ecx

[...]

pop ecx
pop ebx
pop eax
```



Fonctionnement de la pile

Un registre , ESP (Extended Stack pointer) va nous être très utile. En effet, celui ci pointe toujours sur le bas de la pile. Lors d'un transfert (push ou pop) ESP est automatiquement incrémenté ou décrémenté de deux ou de quatre octets.

Mais à quoi la pile va donc nous être utile ?

- appel et retour de fonctions, sauvegarde de registres
- sauvegarde en mémoire afin de libérer des registres (valeurs ou adresse)
- réserver des zones tampons (ou buffers)
- transmettre et récupérer des arguments d'une fonction

résumé

- Si on ajoute un élément sur la pile (on empile), le pointeur ESP sera décrémenté.
- Si on supprime un élément sur la pile (on dépile), le pointeur ESP sera incrémenté.

On ne peut empiler ou dépiler que des valeurs de 16 ou 32 bits soit 2 ou 4 octets. La valeur mise sur la pile s'appelle l'opérande.

Pour revenir à ESP, si on empile une valeur :

- ESP sera décrémenté de 2 dans le cas d'une opérande 16 bits
- ESP sera décrémenté de 4 pour une opérande 32 bits.

Si on dépile une valeur :

- ESP sera incrémenté de 2 dans le cas d'une opérande 16 bits
- ESP sera incrémenté de 4 pour une opérande 32 bits.

La Mémoire

Nous avons vu précédemment que la pile faisait partie de la mémoire mais nous aimerions pouvoir parcourir toute la mémoire. Rappelons que la mémoire est visible sous une forme linéaire, allant de l'adresse 0x0 jusqu'à l'adresse 0xFFFFFFFF. Certaines zones de cette mémoire sont utilisés par le système d'exploitation, les applications (librairies)...

Les modes de fonctionnement:

A) Mode Réel :

Le mode réel est le mode de fonctionnement d'un microprocesseur lorsqu'il démarre (reset ou suite à un arrêt classique).

Le fonctionnement est restreint ainsi que la mémoire disponible (1 Mo, adressage sur 20 bits). Dans ce mode les fonctionnalités sont celles d'un 8086 quel que soit le microprocesseur. Depuis ce mode on peut basculer vers les deux autres modes. Le microprocesseur ne peut exécuter qu'un seul programme à la fois. Le DOS fonctionne dans ce mode.

A l'origine, le 8086 était un microprocesseur avec des registres 16 bits. Ces registres ne pouvaient pas contenir une adresse sur 20 bits. Intel a résolu le problème en segmentant la mémoire en bloc de 64 Ko appelés segment. La valeur de segment peut être stockée dans un registre dédié (CS, DS, ES, FS, GS et SS). Un programme possède en général 3 segments:

- Le segment de code (CS contient l'adresse du segment sur 16 bits)
- Le segment de données (DS contient l'adresse du segment sur 16 bits)
- Le segment de pile (SS contient l'adresse du segment sur 16 bits)

Les autres registres de segment peuvent être utilisés pour différents segments de données.

Entrées		Sortie
a	b	L
0	0	0
0	1	0
1	0	0
1	1	1

fonction logique ET

B) Mode protégé :

C'est le mode que nous utilisons normalement pour nos applications. Toute la mémoire est disponible etc. Dans ce mode, il existe le mode Virtuel 8086 ou V86. Ce mode permet de mettre un environnement 8086 à la disposition d'une application 16 bits.

Ce mode virtuel reste sous le mode protégé. Par exemple, sous Windows on peut ouvrir une session DOS (émulation). Cette session met à disposition 1 Mo de mémoire avec l'environnement DOS complet. A noter que l'on peut ouvrir plusieurs session DOS en même temps. Dans ce mode, nous n'aurons probablement pas à gérer les registres de segment. C'est l'OS qui le fait.

- Modèle multi-segments

Chaque programme reçoit une table de descripteur de segments indépendante (table de descripteurs locaux = Local descriptor table). Chaque segment peut être indépendant de tous les autres segments utilisés par les autres applications (adressage indépendant).

- Modèle paginé :

Dans ce mode, le segment peut être divisé en plusieurs blocs mémoire de 4096 octets appelés page. Ce mode permet d'écrire sur le disque une partie du code qui n'est pas en cours d'exécution. Cela évite de charger l'ensemble de l'application en mémoire. Par contre, avec des ordi ayant peu de mémoire, cela ralentit beaucoup l'exécution. L'OS doit recharger la page de code ou de données si besoin depuis le disque. L'ensemble des pages est aussi appelé mémoire virtuelle et nécessite l'emploi par l'OS d'un gestionnaire de mémoire virtuelle.

C) Mode Gestion système :

Ce mode appelé aussi system management mode. C'est un mode très spécifique réservé à des tâches bien précises comme la gestion de l'alimentation.

Revenons a des exemples pratiques

Si nous voulons transférer le contenu du registre EAX vers l'adresse mémoire 0x12345678 nous ferons :

```
mov    [0x12345678], EAX
```

les crochets [] indiquent que c'est le contenu de l'adresse mémoire.

Supposons maintenant que nous souhaitions passer des arguments à une fonction.

```
        push  1234
        push  ebx
        push  eax
        call  fonction
...

fonction:
        push  ebp
        mov   ebp,esp
        mov   eax,[ebp+8]
        mov   ebx,[ebp+12]
```

Entrées		Sortie
a	b	L
0	0	0
0	1	1
1	0	1
1	1	1

fonction logique OU

```
mov    ecx,[ebp+16]
...
mov    esp,ebp
pop    ebp
ret
```

Dans cet exemple, nous voulons passer le nombre 1234 puis le contenu des registres EBX et EAX. C'est ce que nous faisons avec les trois PUSH. Ensuite viens l'appel à la fonction. Arrivé dans la fonction, nous sauvegardons la valeur de EBP dans la pile puis nous mettons le contenu de ESP dans EBP. Nous nous retrouvons donc avec ,dans EBP, l'adresse du bas de la pile.

Nous faisons ensuite mov eax,[ebp+8] afin de récupérer le premier argument. Alors pourquoi + 8 ? Parce que juste avant,l'adresse de retour a été sauvegardée dans la pile (4 octets) puis nous avons sauvegardé EBP (4 octets).

Nous récupérons donc les trois arguments, puis le programme les traite (les 3 points).

ensuite, on transfert la valeur de EBP dans ESP et on récupère enfin la valeur de EBP que nous avions placé dans la pile au début.

On retourne enfin dans le programme principal, juste en dessous de call.

Les opérations logiques

Si nous voulons changer un bit d'un registre, il nous faut pouvoir manipuler les opérateurs logiques.

Divers opérateurs sont disponibles , nous pourrons utiliser le AND, le OR, le XOR et le NOT.

Le AND

Le ET logique, le AND , fonctionne de la sorte :

Prenons comme exemple un AND entre deux octets :

```
    10010110
AND 00110100
    00010100
```

ce qui donnerait si on voulais faire l'opération en assembleur :

```
    mov    eax,10010110
    and    eax,00110100
```

Nous aurions donc dans eax le résultat 00010100

Le OR

Le OU logique, le OR , fonctionne de la sorte :

Prenons comme exemple un AND entre deux octets :

```
   10010110
OR 00110100
   10110110
```

ce qui donnerait si on voulais faire l'opération en assembleur :

```
    mov    eax,10010110
    or     eax,00110100
```

Nous aurions donc dans eax le résultat 10110110

Le XOR

Le OU logique, le OR , fonctionne de la sorte :

Entrées		Sortie
a	b	L
0	0	0
0	1	1
1	0	1
1	1	0

fonction logique XOR

la seule différence avec le OR est que 1 XOR 1 donne 0 et non 1 comme pour le OR.

Prenons comme exemple un XOR entre deux octets :

```
    10010110
XOR 00110100
    10100010
```

ce qui donnerait si on voulais faire l'opération en assembleur :

```
    mov    eax,10010110
    xor    eax,00110100
```

Nous aurions donc dans eax le résultat 10100010

Le NOT

Le NON logique, le NOT , fonctionne de la sorte :

fonction logique NON

Prenons comme exemple un NOT sur un octets :

Entrée	Sortie
a	L
0	1
1	0

```
NOT 00110100
    11001011
```

ce qui donnerait si on voulais faire l'opération en assembleur :

```
    mov eax,00110100
    not    eax
```

Nous aurions donc dans eax le résultat 11001011

Nous venons de découvrir, les opérateurs logiques en assembleur. Nous verrons dans d'autres articles leur utilité.

conclusion

Nous avons fait , en trois articles un petit tour d'horizon de l'assembleur. n'hésitez pas a récupérer la documentation à l'adresse sitée plus haut. Vous pouvez aussi récupérer la documentation en anglais et compléte (gratuite) à l'adresse suivante :

http://www.intel.com/design/pentium4/manuals/index_new.htm

bonne lecture...

Paramétrer son ro

Les providers actuels proposent maintenant des accès internet « tout en un » intégrant le modem ADSL, un routeur et même maintenant la téléphonie sur internet. Tous offre une aide à l'installation mais pour le commun des mortels, cela peut paraître compliqué. Pour le coup quelques explications techniques sont nécessaires....:-)

On voit maintenant partout arriver chez nos providers des « machinesbox », free ayant le premier lancé la mode de ce type de connexion à l'Internet.

Il en existe en fait de deux sortes, celles qui se paramètrent via une page web perso chez votre provider (typique chez Free) et celles qui ont leur propre interface web d'administration permettant de les configurer directement(elles ont ma préférence en ce qui me concerne).

Ces « accès boxes », intègrent beaucoup de fonctions qui vous évitent l'utilisation d'un PC, mais qu'il est nécessaire de comprendre.(modem-routeur-téléphonie)

Dans l'absolu un routeur a deux fonctions principales:

• Partager une connexion Internet aux différents utilisateurs d'un réseau de manière fiable

• Sécuriser ce réseau en régulant le trafic d'informations entrant et sortant d'Internet.

Le routeur, comme son nom l'indique, fait transiter des paquets d'informations entre le réseau privé et internet.(cf Acheminement des données vers le FAI)) Pour résumer, c'est un guide : vous lui demandez votre route, il vous accompagne vers la bonne destination. Sa fonction principale est de prendre un paquet et de le renvoyer au bon endroit en fonction de la destination finale.

Un routeur se compose généralement:

• d'une interface WAN qui permet de connecter le modem ADSL/Câble. Dorénavant les routeurs/modem ADSL se généralisent.

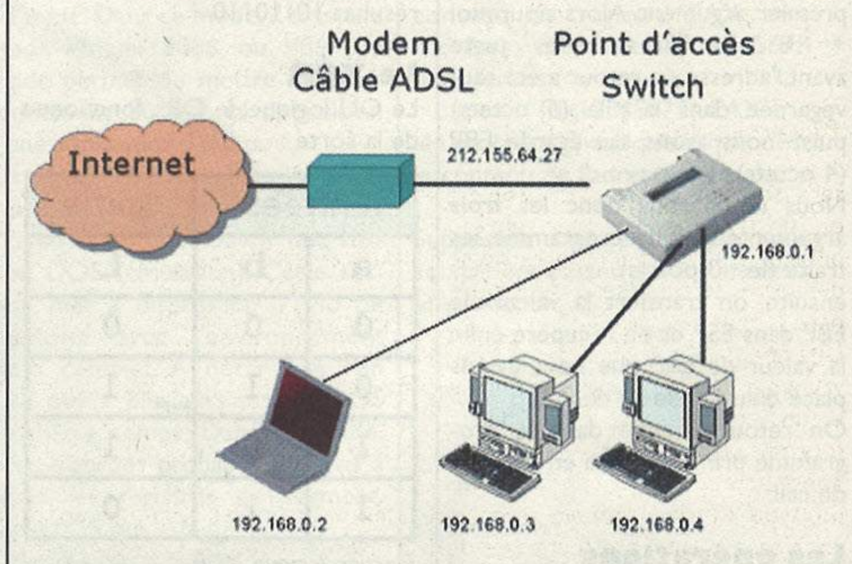


Schéma du réseau avec routeur

• d'une ou de plusieurs interfaces réseau local (LAN) :

1. Ethernet : Quelquefois le routeur intègre aussi un mini switch 10/100, c'est à dire une série de prises réseau classiques RJ45.

2. Éventuellement des interfaces :USB, BlueTooth, Wifi, Courant Porteur.

• Enfin les plus récents intègrent un module de téléphonie sur ip (TOIP)

Sur Internet, votre FAI vous assigne une adresse IP publique qui vous identifie sur le réseau, c'est votre routeur qui récupère cette adresse. Votre routeur peut également attribuer une adresse IP (privée) aux ordinateurs auxquels il est relié.(DHCP)

Commençons dès maintenant l'installation de notre routeur, nous parlerons d'un routeur intégrant une interface web d'administration. L'appareil étant correctement connecté (cf doc constructeur), ouvrez un navigateur web et tapez comme URL l'adresse ip mise par défaut(cf notice installation), elle

teur correctement

Informations modem
Configuration avancée
Réseau sans fil
Voix
MGCP
Diagnostique
Gestion

Voice – MGCP configuration
Enter the MGCP related parameters

Click "Stop MGCP client" before changing the parameters and click "Start MGCP client" to save the MGCP parameters.

Call Agent IP Address/FQDN	mgc1.tiscali.fr ou mgc2.libertysurf.net
MGCP client name	20 caractères.mgcp
AALN	1
Interface name	ppp_8_35_1 · pppoe_8_35_1
Preferred codec	Auto
Country setting	France
Call Agent port number	2427
MGC port number	2427
TX Gain	0 dB
RX Gain	0 dB
PSTN access code	**
Heartbeat Time	60
Emergency List	

Start MGCP client

Stop MGCP client

Paramètrage téléphonie

sera souvent du type 192.168.1.1 ou 0.1.(vous aurez pris soin au préalable de vérifier que l'adresse de votre carte réseau se trouve dans la même classe d'IP)

Une fenêtre d'authentification s'ouvre alors et vous demande un login et un mot de passe prédéfinis et fournis par votre FAI ou le constructeur qui est généralement du type « admin, admin » ou « root, pass » enfin bref à changer de suite car c'est une faille de sécurité plus souvent rencontrée que l'on ne croit ;-)

La première chose à paramétrer est le WAN (wide Aréa Network) c'est à dire notre accès à l'internet. Vous devez renseigner les paramètres suivants:

I Le VPI (virtual path) et le VCI (virtual channel identifier) de valeurs respectives 8 et 35(cf encadré ATM)

- Le choix du protocole réseau soit le PPPoA ou le PPPoE et le mode d'encapsulation VC/MUX en fonction des instructions de votre provider.
- Votre login et mot de passe fourni par le FAI
- Vous devrez également vérifier pour certains routeurs que le protocole IGMP(internet Group Management Protocol) est validé ainsi que le Wan Service.

Pour les modems intégrant la téléphonie(cf encadré), vous devez maintenant la paramétrer, allez sur l'interface gérant la téléphonie (voix ou voice) et commencer par arrêter le client MGCP.

Les champs les plus importants à renseigner sont :

- Le Call Agent IP (prestataire), par exemple rtp.voip.club-internet.fr
- Le MGCP client name (code confidentiel fourni)
- Vérifier le champ Preferred Codec (sur auto)
- Le Country Settings (France)
- Le Call Agent Port Number(2427), le port par lequel passera votre téléphonie.
- Le MGC Port Number (2427)
- Enfin on vous conseillera de laisser le TX/RX Gainà 0db

Vous vérifierez également à ce stade que la passerelle de votre FAI est bien déclarée, en fait il vous suffira dans de nombreux cas de cocher une case disant au routeur d'utiliser la « GateWay » envoyée par votre FAI.

Voilà votre routeur est opérationnel sur son réseau externe, n'oubliez pas de changer le couple login-mot de passe, généralement dans une section management-security.

Vous devez maintenant vous préoccuper du réseau interne (privé), toujours dans l'interface d'administration, cherchez un onglet « Lan » ou similaire.

Vous pouvez maintenant changer l'adresse ip privée du routeur et activer le serveur DHCP(Dynamic Host Configuration Protocol) qui vous permettra d'affecter automatiquement une adresse ip, un masque de sous réseau, une passerelle et un ou des DNS, à chacune de vos machines, vous devez simplement définir la plage d'adresses que vous désirez octroyer.(déterminer là en fonction du nombre de machines de votre réseau)

Exemple de configuration Lan:
Adresse routeur: 192.168.1.1
Masque de sous réseau: 255.255.255.0
Début de la plage d'adresses du serveur DHCP: 192.168.1.10
Fin de la plage d'adresses du serveur DHCP : 192.168.1.20
Durée du bail: 24h

Sur certains routeurs vous pouvez même affecter les adresses IP en fonction des adresses matérielles des cartes réseau (Mac Adress)

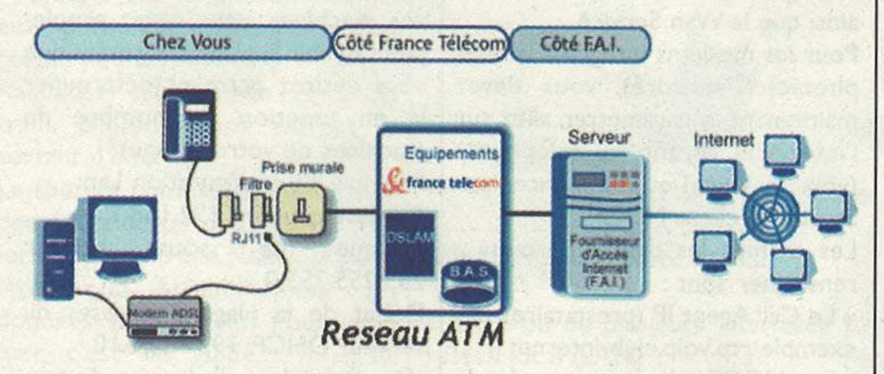
D'autres intègrent une deuxième interface lan vous permettant de créer un deuxième réseau privé.

Bon votre routeur étant compatible wifi, il va falloir maintenant le configurer; allez dans la section

Utilisée par France Télécom, la liaison ATM est une liaison Point à point qui achemine les paquets PPP jusqu'au BAS en passant par le DSLAM (cf.figure Acheminement des données...) Au-delà du BAS, c'est une liaison ethernet haute vitesse qui relie le BAS au Fournisseur (protocole L2TP, Serveurs Radius).
Le DSLAM (Digital Subscriber Line Acces Multiplexor) réalise l'interface entre les lignes ADSL et le réseau d'accès. Il assure :
- le raccordement des lignes ADSL.
- la séparation de la bande de fréquences téléphoniques et de la bande de fréquences des données.
- la fonction modem ADSL. (en clair, le dslam est une armoire contenant des cartes qui sont des modems communiquant avec celui de l'utilisateur)

Le BAS (Broadband Acces Server) réalise l'interface entre le réseau de collecte des lignes ADSL et les réseaux d'accès aux fournisseurs d'accès Internet. Il remplit entre autres les fonctions suivantes :
- première authentification des clients.
- routage des données vers les différents fournisseurs d'accès

Le choix des protocoles dépend de l'opérateur et du FAI, PPPoA et PPPoE RFC1483 bridge mode,VPI/VCI 8,35.
• PPPoA = PPP (Point to Point Protocol, internet) over ATM (asynchronous transfer mode). Les données sont transportées par "cellules" dans un "canal virtuel" identifié par le couple VPI/VCI
• PPPoE = PPP over Ethernet over ATM.Il n'y a pas de supériorité d'un protocole sur l'autre en terme de performance. En théorie PPPoA est + rapide, dans la réalité, c'est l'optimisation des réglages du système d'exploitation qui aura une influence significative



Acheminement des données vers le FAI

« wifi » ou « wireless » de votre routeur et commencez par activer cette fonction puis entrez votre ESSID (Extended Service Set Identifier) généralement abrégé en SSID qui sera en fait le nom de votre réseau. Il existe une fonction permettant de cacher le nom de votre réseau(Hide SSID), cochez là, ce sera une première mesure de sécurité. Votre routeur wifi vous permet également de choisir la norme wifi, la norme en cours 802.11g permet la connection des clients 802.11b et g, choisissez là.
Le mode wifi vous permet également de filtrer les clients par leur adresse MAC cela vous donnera un niveau de sécurité supplémentaire.(sous windows en mode console==>ipconfig/all et sous linux ifconfig vous renseignerons sur celle -ci)
Nous allons maintenant définir le mode d'authentification:
Vous avez plusieurs possibilités, mais pour une sécurisation minimale de votre réseau activez le chiffrement WEP en mode restricted uniquement et choisissez une longueur maximale de clé de 128 bits. Certains routeurs vous permettent de définir vos clés WEP en fonction d'une « passphrase »
Pour une meilleure sécurité et si votre équipement le permet, choisissez le chiffrement WPA PSK ou WPA2 , WPA Enterprise nécessitant un serveur Radius.(Les expliquer ici serait trop long et cela fera l'objet d'un prochain article)
Si nous récapitulons notre routeur est maintenant configuré coté WAN, LAN téléphonie et WIFI mais comment nos machines dotées d'adresses privées communiquent avec le monde extérieur?
Un routeur, comme son nom l'indique, redirige les paquets qu'il reçoit en fonction d'une table de routage vers le routeur suivant jusqu'à atteindre le réseau local de destination. Chaque paquet comporte l'adresse d'origine et l'adresse de destination. Dans le cas d'adresses privées, l'adresse d'origine est une adresse privée inconnue de l'Internet. Le destinataire ne pourra pas répondre. Il faut donc remplacer l'adresse privée d'origine par une adresse publique. C'est le travail du routeur NAT (Network Address Translation) qui effectue la transformation des adresses. Pour pouvoir configurer correctement un routeur NAT, il faut comprendre la notion de port.
Le protocole TCP/IP utilise des ports (un nombre de 0 à 65535) comme le moyen de nommer les bouts d'une connexion logique, une conversation qui comporte plusieurs échanges. Les ports permettent de réaliser simultanément des milliers de connexions logiques sur la même adresse IP. Ils permettent de partager la liaison Internet

La voix sur réseau IP, parfois appelée téléphonie IP(TOIP)ou téléphonie sur Internet, et souvent abrégée en « VoIP » (abrégé de l'anglais Voice over IP), est une technique qui permet de communiquer par voix à distance via le réseau Internet, ou tout autre réseau acceptant le protocole TCP/IP.
Au contraire des téléphones analogiques filaires (RTC) dépendant de centraux téléphoniques dédiés, la voix sur IP permet le transport de conversations téléphoniques sur tout réseau numérique ou analogique acceptant le protocole TCP/IP (Ethernet, RNIS, PPP, etc.)
Les trois principaux protocoles utilisés pour l'établissement de connexions en voix sur IP sont :

- Le protocole H323, c'est le plus connu et se base sur les travaux de la série H.320 sur la visioconférence sur RNIS. C'est une norme stabilisée avec de très nombreux produits sur le marché (terminaux, gatekeeper, gateway, logiciels). Il existe actuellement 5 versions du protocole (V1 à V5).
- Le protocole SIP est natif du monde Internet (HTTP) et est un concurrent direct de l'H323. A l'heure actuelle, il est moins riche que H.323 au niveau des services offerts, mais il suscite actuellement un très grand intérêt dans la communauté Internet et Télécom.
- Le protocole MGCP est complémentaire à H.323 ou SIP, et traite des problèmes d'interconnexion avec le monde téléphonique (SS7, RI).MGCP(Media Gateway Control Protocol) est un protocole asymétrique(client-serveur) de VoIP.

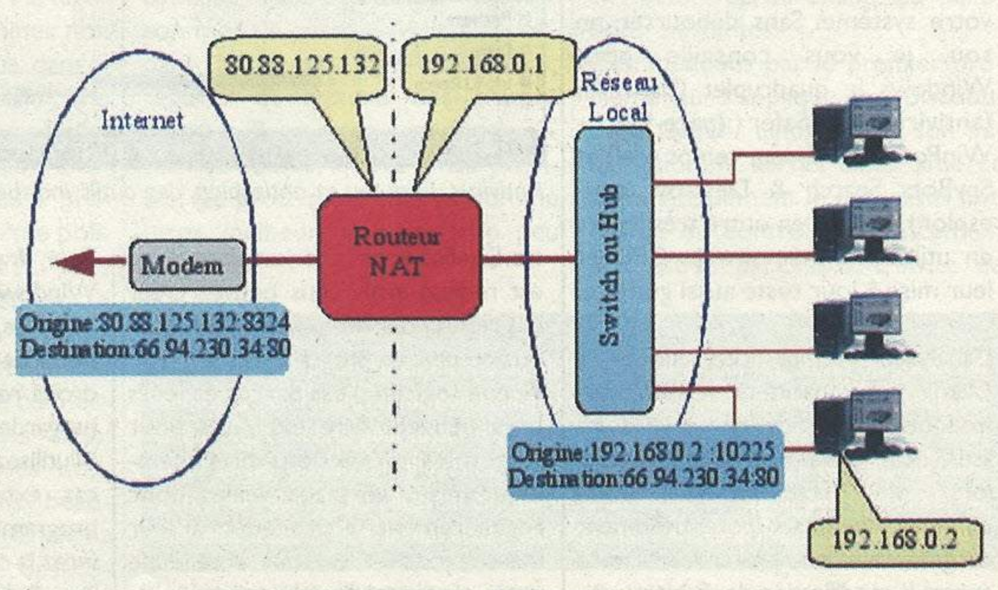
Les FAI par ADSL Français utilisent en général ce protocole pour la téléphonie(le serveur, un SoftSwitch, contrôle le téléphone de l'abonné).

entre des programmes différents et des machines différentes à la maison. Comme pour les adresses IP, l'IANA a classé les ports en 3 catégories. De 0 à 1023, les "Well Known" ports utilisables seulement par le système ou des fonctions associées, de 1024 à 49151 les "Registered" ports utilisables par les programmes utilisateurs, de 49152 à 65535 les ports dynamiques ou privés. Par défaut, le protocole http utilise le port 80, le POP3 le port 110, etc...
Lorsqu'une machine du réseau local envoie des paquets à un serveur à l'extérieur, l'adresse d'origine est une adresse privée. Le destinataire ne pourra pas répondre à cette adresse. Pour résoudre ce problème, le routeur NAT remplace l'adresse et le port d'origine par l'adresse Internet publique du routeur et un numéro de port libre choisi au hasard en notant adresse et port associés à la machine locale (cf figure translation d'adresse réseau).
La machine de destination renvoie la réponse sur l'adresse et le port visible de l'Internet au routeur NAT. Celui-ci fait alors la transformation inverse pour renvoyer les paquets vers la machine locale. Dans ce cas de figure, il n'y a rien de spécial à configurer. C'est comme cela que fonctionnent les messageries instantanées. Le logiciel de la machine sur le réseau privé se connecte au serveur de messagerie qui connaît ainsi l'adresse externe et le numéro de port du routeur qui permet de contacter cette machine.
En revanche, une machine qui appelle depuis l'Internet pour atteindre une adresse privée n'a aucun moyen d'y arriver puisque le routeur ne sait pas sur quelle machine du réseau Interne, il faut router l'appel. Il existe un moyen qui s'appelle port forwarding, cela fera l'objet du prochain article où nous aborderons les fonctions de Port-Forwarding, Port Triggering, DYNDNS,UPNP,QOS et bien d'autres encore dont sont capables les routeurs actuels.

Quelques adresses utiles:

http://www.portforward.com/routers.htm
(un site sur le paramètrage de nombreux routeurs)
http://www.commentcamarche.net/internet/nat.php3

ReZoR



La translation d'adresse réseau

Comment protéger sa machine jusqu'au bios

Les programmes espions, virus et autres sont de plus en plus nombreux. Dans cet article, Net Secret's vous explique comment réduire au maximum le succès de ces attaques, en partant du principe que l'agresseur est prêt à tout...

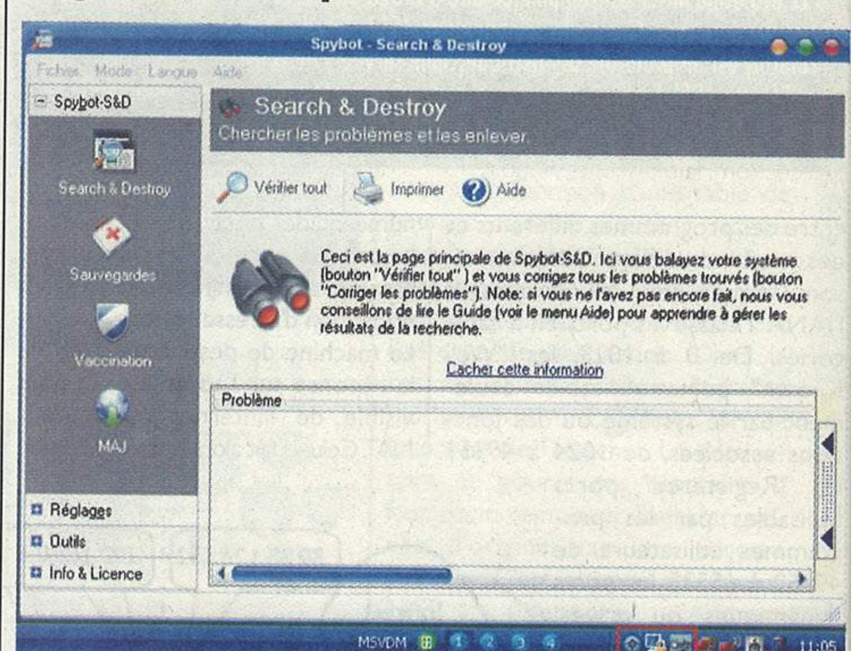
INTRODUCTION

La manière la plus simple, et la plus discrète, de s'en prendre à votre machine est de lui faire exécuter un programme à votre insu qui peut détruire, envoyer diverses données personnelles vers un serveur distant, ou encore ouvrir une "backdoor", "porte de derrière" en bon français, pour une prise de contrôle directe par l'attaquant.

Les logiciels indispensables

La première barrière consiste à un trio de programmes devenus indispensables de nos jours : anti-virus, pare-feu et anti-espion. Cependant, il faut bien les choisir car nombre d'entre-eux n'en portent que le nom, s'affichent polyvalents, mais ne font que ralentir considérablement votre système. Sans débourser un sou, je vous conseille pour Windows le quadruplet ClamWin (antivirus) - iSafer (pare-feu) - WinPooch (analyseur temps réel) et SpyBots Search & Destroy (anti-espion). Ils sont en outre très légers en utilisation mémoire et CPU et leur mise à jour reste aussi gratuite.

L'analyseur temps réel ajoute à ClamWin la capacité de vérifier automatiquement les fichiers que vous utilisez, mais également l'avertissement lors de l'établissement d'une connexion réseau potentiellement dangereuse et une protection efficace contre la modification des fichiers critiques du système et de la base de registre. En effet, votre autorisation explicite est requise, mais vous pouvez créer des règles pour définitivement bloquer ou accepter un programme.

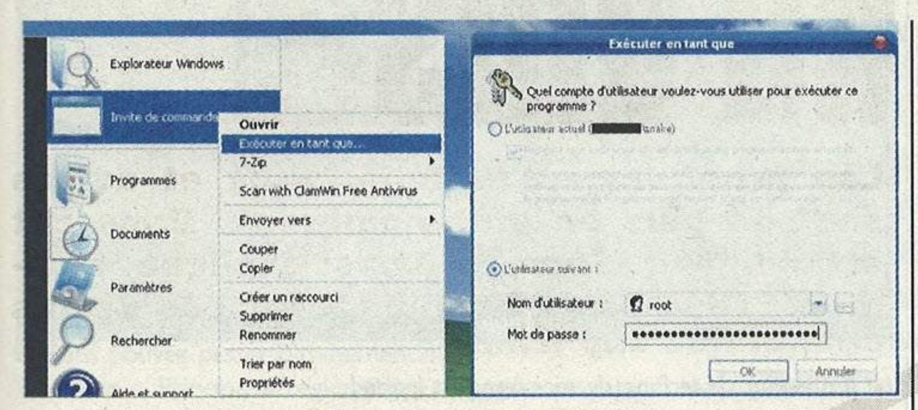


Antivirus, pare-feu et antiespion, des outils indispensables...

Aucun logiciel n'est parfait et leurs bugs peuvent être exploités pour passer les protections précédemment mises en place. Veillez donc régulièrement à procéder à leur mise à jour, et surtout à celle de votre système d'exploitation et de votre navigateur Internet.

Pour frapper un grand coup sous Windows et ainsi bloquer les attaques les plus malicieuses, inspirons-nous de GNU /Linux : donnez les droits restreints à vos utilisateurs et ne gardez qu'un utilisateur privilégié. N'utilisez cet utilisateur que dans des cas extrêmes, (dés)installation de programmes ou de matériels, et préférez la commande "Exécuter en tant que..." disponible par clique-droit sur les raccourcis et les exécutables.

machine de l'Internet



Application de la stratégie des utilisateurs de GNU / Linux sous Windows...»

Désormais l'infection automatique est écartée au maximum. C'est à vous de jouer pour compléter cette protection : faîtes très attention aux fichiers que vous ouvrez / exécutez et où vous surfez. De nombreux sites peu recommandables réduiront à néant l'efficacité de votre trio si vous avez le malheur de lancer un de leur programme.

Le réseau local

Descendons maintenant d'un niveau : le réseau local. Partager des fichiers avec des machines non protégées est encore plus dangereux qu'avec Internet. En effet, une trop grande confiance est facilement accordée aux données transitant entre deux ordinateurs proches. Appliquez donc la même politique à tous vos réseaux et si vous utilisez le WIFI, chiffrez votre connexion en WEP ou en WPA de préférence, pour empêcher un ordinateur extérieur de se connecter. Malheureusement, ces deux algorithmes ont été cassés mais cela demande néanmoins beaucoup de temps en WPA. Changez donc régulièrement de clé, désactivez les services que vous n'utilisez pas et remplacez les moyens de communication non sécurisés par leurs équivalents qui le sont, comme Telnet par OpenSSH, par exemple. Supprimez les comptes par défaut et mettez des mots de passe. Pensez à vos partages réseaux !

Nous sommes désormais à un point où il devient très difficile d'attaquer à distance. C'est la qualité de vos mots de passe qui joue désormais, confère encadré "Choisir son mot de passe...". Veillez cependant à ne pas être espionné : regards et lecture des trames réseaux. Pour cette seconde éventualité, utilisez, quand c'est possible, les protocoles chiffrés comme https, malheureusement trop peu proposés.

Mettre des mots de passe c'est très bien, mais ne quittez pas votre poste sans verrouiller votre session. En effet, quelqu'un pourrait intervenir sur votre système pendant votre absence et mettre à mal tous vos efforts. Pour parer à l'oubli, et limiter la durée de vulnérabilité, activez l'écran de veille automatique avec un laps de temps minimum et équipez-le de la demande du mot de passe utilisateur.

Le démarrage

À cet instant, votre ordinateur semble blindé, mais sa plus grande faille reste le démarrage. Il est possible, d'une part, de configurer les options de lancement des systèmes d'exploitation, et d'autre part, il est de nos jours possible de démarrer sur une large gamme de périphériques (disques durs, disques optiques, disquettes, clé USB, ...) pour lesquels il existe des mini systèmes d'exploitation capables d'intervenir en lecture/écriture sur les partitions existantes.

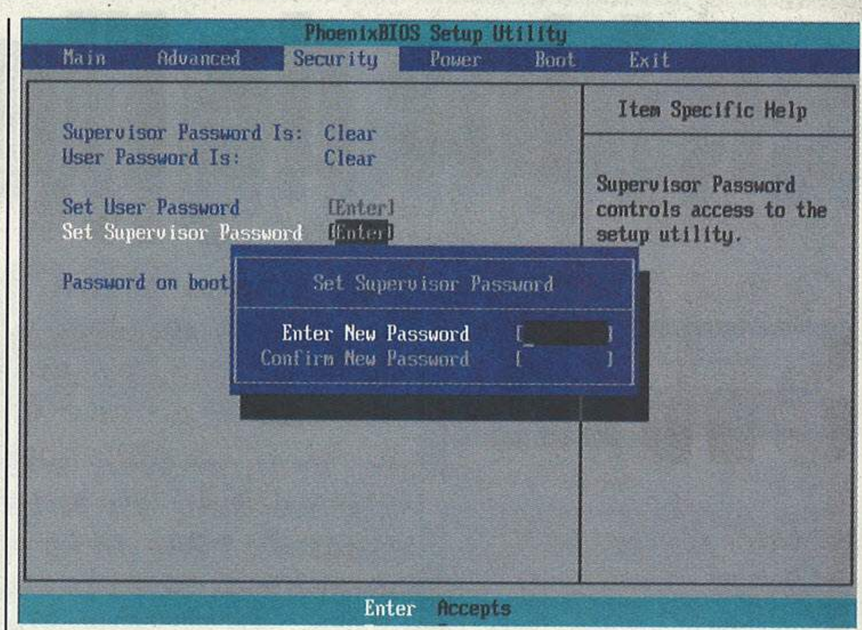
Commençons par le premier problème qui s'applique aux distributions GNU / Linux. Après son initialisation, le kernel Linux amorce automatiquement le processus Init, chargé du contrôle du lancement des autres processus. L'invite de

Un bon mot de passe est en théorie un mélange subtil de chiffres, lettres majuscules et minuscules et d'autres caractères comme #,@,$,... Bref quelque chose qui ne veut rien dire car les utilitaires pour casser les mots de passes se basent sur des dictionnaires. N'en créez surtout pas de compliqués car d'une part le risque d'oubli est fort, mais d'autre part si vos utilisateurs l'écrivent en clair dans un fichier ou sur un post-it, cela ne sert strictement plus à rien. Il vaut donc mieux faire plus simple mais en changer souvent...

Choisir son mot de passe...

connexion apparaît alors et seul les utilisateurs authentifiés ont un accès au système. Il est cependant possible de remplacer init par un programme de son choix en éditant la ligne des options passées au kernel à l'invite du chargeur de démarrage. C'est ainsi que la simple addition de "init=/bin/sh" donne une invite de commande en root, administrateur suprême sous GNU / Linux, sans aucune authentification au préalable. L'ajout d'un mot de passe de modification au chargeur de démarrage est donc primordial !

Continuons avec le second problème, qui peut se résumer aux ennuies des accès inter-systèmes d'exploitation. Si vous possédez plusieurs systèmes d'exploitation en multiboot, veillez à ce que les droits soient homogènes entre eux. En effet, un utilisateur ayant plus de droits sur l'un pourrait provoquer une élévation de privilèges sur l'autre. La seule solution pour se prémunir des mini-distributions, c'est de tenter d'empêcher leur lancement. Rendez-vous alors dans le bios, mettez un mot de passe à son accès et positionner en premier votre disque dur de démarrage dans l'ordre d'amorçage des unités. Attention : certains bios récents proposent d'afficher un menu pour choisir son unité de démarrage, ce qui rend inutile la



La protection via le Bios, dernier rempart logiciel...

précédente manipulation. Si vous êtes dans ce cas, vous devez activer le mot de passe du bios également au niveau du boot.

CONCLUSION

Voilà, désormais votre machine est plus sécurisée et prête à faire face aux principales menaces durant les longues soirées d'hiver. Vous avez pu constater par vous même que chaque parade mise en place pouvait être contrée. Même la dernière, où l'ouverture de l'unité centrale permet une remise à zéro du bios, donc du mot de passe associé, et ainsi la remontée de la chaîne de protection. Son enfermement dans un coffre fort n'arrangerait rien puisqu'il existe des mots de passe standards et des outils pour trouver les vôtres. Rien n'arrêtera un pirate prêt à tout. Vous ne pouvez que le ralentir. Sachez tout de même qu'à moins que vous possédiez quelque chose ayant un réel intérêt pour lui, il préféra trouver une victime plus facile quand il constatera les toutes premières protections mises en place.

SnAkE

Votre système est plus lent que d'habitude, vous constatez une activité inhabituelle sur votre disque dur ou de votre réseau, votre PC est alors sûrement infecté. Mettez à jour votre antivirus et (installez) Spybots Search & Destroy. Redémarrez en mode sans échec, puis lancez un scan complet du système pour supprimer virus et espions. Recommencez cette étape autant de fois que nécessaire pour tout supprimer. Si au bout de cinq redémarrages des intrus subsistent, c'est qu'ils sont sûrement installés en tant que services. Lancez alors msconfig et rendez-vous dans l'onglet services. Cochez "cacher les services Microsoft". Vous serez alors en mesure de repérer très facilement les intrus. Décochez-les et validez. Relancez les scans pour les supprimer définitivement.

La protection via le Bios, dernier rempart logiciel...

AntiVirus ClamWin : http://fr.clamwin.com
Analyseur temp réel pour ClamWin WinPooch : http://winpooch.free.fr
AntiEspion SpyBots Search & Destroy : http://www.safer-networking.org
Pare-Feu iSafer : http://winsockfirewall.sourceforge.net
OpenSSH : http://www.openssh.com

Les adresses des outils mentionnés dans l'articles

GRAND CONCOURS SWIR

Nous lançons un grand concours de conception de site web à l'aide d'un tout nouveau CMS, en gros, un outil de gestion de contenu de site web. Celui-ci est assez récent et sa philosophie est différente des autres CMS que vous pouvez trouver. Cet article va vous détailler l'histoire de SWIR, les modalités du concours et l'installation ainsi que son fonctionnement.

Histoire d'un petit CMS

Pour ceux que l'histoire ennuie, il n'est pas utile de lire cette partie de l'article et vous pouvez passer directement à la section « Principe et règlement du concours ». Pour les autres qui aiment connaître les origines et la façon dont est né un concept ou un produit, je vous invite à lire la suite. Je vais vous raconter l'histoire qui m'a amené à écrire SWIR.

Il m'est souvent arrivé que des amis, peu connaisseurs en informatique et en conception de pages web, me demandent de les aider à concevoir leur site pour une association, pour une mairie ou simplement pour leur utilisation personnelle. Dans cette situation deux possibilités s'offraient à moi; soit je faisais le site et très vite j'étais sollicité quotidiennement pour changer ceci ou cela; soit je les formais à l'utilisation d'un outil, et là, j'en avais pour plusieurs semaines voir plusieurs mois si l'utilisateur est vraiment grand débutant en informatique. Car, en effet, pour une personne qui utilise son ordinateur pour jouer ou faire quelques dessins ou lettres, la conception de pages web bien faites, ressemble au parcours du combattant! Il faut comprendre un tas de mots barbares comme HTML, FTP, CSS, <a href.... , avoir une bonne vision de l'arborescence du futur site, ranger de façons ordonnées tous les fichiers... Bref, pour former une personne rapidement, on se tourne très généralement vers des logiciels de wysiwyg (What You See Is What You Get) qui, en principe, ne demandent pas de connaissances particulières en HTML ou autre PHP, JSP, Perl... Mais l'utilisateur non averti va faire des pages sans respecter une charte graphique et une hiérarchie des données. Au bout de quelques semaines, il vous appelle au secours et vous trouvez une tonne de fichiers dans tous les sens et sans aucune organisation sur son ordinateur. C'est souvent le résultat de beaucoup de copier/coller et glisser/déplacer. Ça devient un vrai casse tête pour vous de tout retrouver et de tout ranger. En plus, le problème risque de se poser plusieurs fois avant que la personne ne devienne réellement autonome sur la conception de son site. Une autre catégorie d'outils qu'il est intéressant d'exploiter, sont les CMS. Là, on vous donne un site clef en main. Il vous suffit de déposer l'ensemble des fichiers sur un serveur, ce que vous pouvez faire rapidement pour votre copain, puis de répondre à quelques questions et en quelques minutes, le site est en ligne. Vous pouvez ensuite passer quelques heures à lui expliquer le maniement des fonctions principales, et ça y est, vous vous dites qu'il est autonome. Et bien vous vous trompez, car l'expérience m'a montré qu'il va oublier une bonne quantité des choses que vous avez faites avec lui, et c'est humain. Ce serait la même chose si on apprenait à un informaticien la calibration d'une fluorescence X en une heure. Donc, il vous rappelle, et comme vous êtes un féru d'informatique sympa, vous ne le laissez pas tomber, vous allez le dépanner. Puis, il vous demande comment customiser tel ou tel truc, et mettre une image là, et un logo ici... HAAaaaa!! c'est de nouveau le casse tête. Vous vous dites qu'avec tout ce qu'on vous demande pour la conception des sites web, vous allez pouvoir ouvrir votre boîte et que c'est certainement pour cette raison qu'il en existe tant sur le marché. En plus elles demandent des sommes assez rondelettes. Mais vous savez que votre copain n'a pas beaucoup d'argent, c'est juste pour sa petite association de motos, et puis vous vous voyez mal lui demander de l'argent car c'est un bon copain et vous êtes un mec bien.

Toutes ces réflexions me poussaient à me dire qu'il serait bien d'avoir un outil simple pour concevoir des sites, et qui ne regorge pas trop de fonctions. J'ai cherché et testé beaucoup d'outils, et j'en ai

trouvé des merveilleux. J'en profite pour féliciter tous ces programmeurs du monde du libre qui donnent de leur temps et qui nous offrent tous ces Nvu, NPDS, Mambo, Plone, ZOPE... Mais malheureusement, ces outils semblent encore trop compliqués pour beaucoup de monde. C'est alors qu'un industriel Luxembourgeois, PDG de plusieurs entreprises, me demanda de lui concevoir un site pour sa société. Il ne voulait pas quelque chose de trop compliqué. C'est un utilisateur de l'outil informatique, mais qui n'a pas le temps de se préoccuper des détails de programmation et de langage HTML, peut-être comme vous. Il parcourt le monde et voulait pouvoir rapidement mettre en ligne une page sur un chantier afin d'informer ses clients, et ceci, en disposant d'une simple connexion internet sans aucun autre logiciel propriétaire. Comme c'est un très bon copain et un membre bienfaiteur de la Team AC'ISSI, je me suis donc dit que j'allais lui faire un système d'administration pour son site en ligne dans un simple navigateur web. Je me suis alors fixé les contraintes suivantes :

- toute l'administration du site doit se faire dans un navigateur
- le système doit proposer des pages types avec juste quelques champs à compléter
- l'administration d'un menu et de sous-menus doit être simple
- la liaison des pages aux liens des menus doit se faire intuitivement
- On doit pouvoir sauver l'ensemble des pages du site à un instant donné et pouvoir les restaurer ultérieurement.

Après quelques mois de programmation sur mon temps libre et la mise au point de plusieurs versions, SWIR à maintenant plus d'un an et est entièrement sous licence libre (GNU GPL).

Vous pouvez télécharger la dernière version 0.2.6.2 sur :

http://acissi.net/swir

Principe et règlement du concours

Pourquoi ce concours?

Le concours qui vous est proposé ici a plusieurs objectifs :

Premièrement : Tester l'outil SWIR (Site Web à Implémentation Rapide) dans le cadre de la création rapide d'un site web. Trouver les dysfonctionnements, les manques d'ergonomie et proposer des remédiations éventuelles.

Deuxièmement : Trouver un design qui sort de l'ordinaire pour le site du magazine, tout en respectant la charte graphique, et une organisation originale des rubriques que vous pensez intéressantes.

Troisièmement : Vous faire gagner une PSP ;-)

L'appréciation des sites réalisés tiendra compte de l'aspect graphique, de l'organisation des rubriques et de la compétence technique qui aura néanmoins une importance moins grande dans le but de laisser la chance à tous de gagner. L'esprit de SWIR étant justement de pouvoir réaliser des sites avec des connaissances minimes voir nulles en programmation Web.

Le règlement

article 1

Les candidats doivent nous informer par mail à grandconcoursswir@acissi.net de leur participation au concours avant le 31 octobre 2006. Le mail doit préciser : le nom, le prénom, l'adresse postale, et l'âge du candidat ainsi que l'URL à laquelle le site est visible sur internet.

article 2

Le site proposé devra obligatoirement être réalisé à l'aide de SWIR qui est librement téléchargeable sur http://acissi.net/swir .

article 3

Toute modification du code source de SWIR devra nous être communiqué par mail à swir@acissi.net afin respecter la licence GPL.

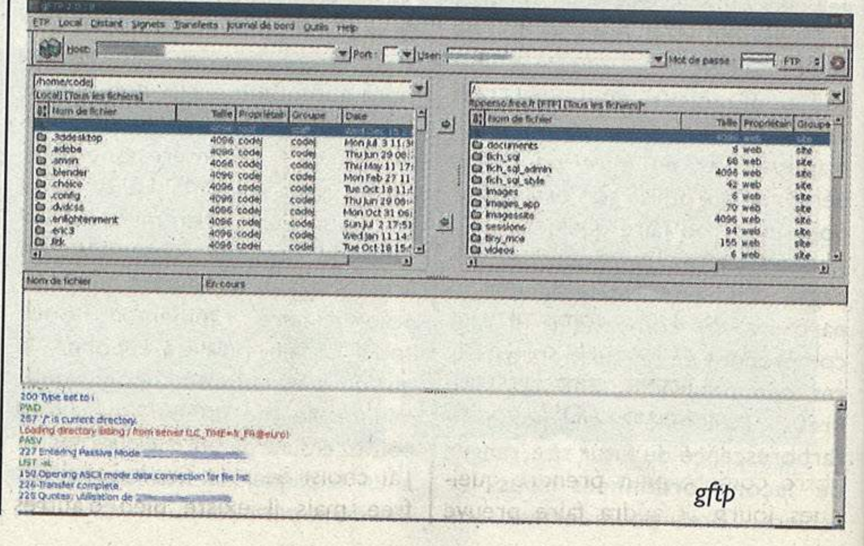
article 4

La page d'accueil du site présenté au concours devra contenir obligatoirement le texte suivant : « Ce site n'est pas le site officiel de Net Secret's, mais, est uniquement destiné à la participation au grand concours SWIR de septembre 2006 organisé par ce magazine. Les pages officielles de Net Secret's sont sur http://acissi.net »

article 5

Le site proposé ne devra plus changer après le 30 novembre 2006 en vue d'être examiné par notre jury.

Télécharger



gftp

et installer SWIR

Où trouver SWIR

Vous pouvez trouver SWR en libre téléchargement dans sa version 0.2.6.2, sur notre site http://acissi.net/swir rubrique téléchargement. Il est proposé au choix sous la forme d'une archive zip, plus orientée pour les utilisateurs Windows ou un archive tar.gz pour les utilisateurs de Linux. Ces deux archives contiennent exactement les mêmes fichiers.

Hébergé gratuitement votre site

Pour fonctionner, SWIR a besoin que votre serveur ou votre hébergeur supporte le PHP avec ouverture de session et dispose d'une base de données MySQL. Pas de panique, pour ceux qui ne comprennent pas ce charabia, nous allons voir ensemble comment faire fonctionner tout ça gratuitement. Pour les utilisateurs plus avertis, vous pouvez passer cette rubrique et vous rendre au paragraphe suivant « Installer SWIR ».
Donc, pour ceux qui sont encore avec moi, je vous propose de créer un compte chez free. En effet, ce prestataire propose gratuitement tout ce dont nous avons besoin pour faire fonctionner SWIR. Si vous disposez déjà d'un compte chez free, vous pouvez en créer un supplémentaire attaché à votre compte principal pour la réalisation de votre site. Pour les autres, il faut dans un premier temps créer un compte principal en cliquant sur « inscrivez-vous » sur la page http://subscribe.free.fr/accesgratuit/ . Suivez les 4 étapes que free vous propose. Même si free vous propose encore une connexion bas débit, grâce à ce compte, vous n'êtes absolument pas obligé de l'utiliser et il faut au contraire utiliser votre connexion ADSL, si vous en disposez d'une. La validation de votre compte peut prendre quelques jours. Il faudra faire preuve d'un peu de patience.
Une fois ce compte principal créé, il nous reste encore à créer un compte supplémentaire qui vous permettra de choisir un nom sympathique à votre site et de l'effacer éventuellement sans toucher à votre compte principal. La procédure est la suivante :

- identifiez-vous en vous connectant avec votre compte principal sur le site http://free.fr
- cliquez sur « Créer vos comptes emails supplémentaires »
- indiquez alors le nom du compte que vous voulez créer. Par exemple, votre prénom un point et concoursswir. Puis, donnez un mot de passe pour ce compte.

Voilà, votre nouveau compte est créé et free vous indique qu'il sera actif dans 2 heures environ. C'est souvent un peu plus, voir le lendemain. Une fois celui-ci actif, la procédure n'est pas entièrement finie et il va vous falloir encore un peu de patience. Je sais que tout ça peut vous paraître long, mais vous y trouverez un confort de travail. Pour l'instant, vous avez un nouveau compte mail et il faut activer les pages personnelles pour celui-ci. La démarche est la suivante :
identifiez vous sur free avec le compte pour lequel vous voulez construire des pages
cliquez sur « Activer votre compte pour les pages personnelles »

- à ce moment, il ne faut pas oublier de cocher la case « Activer ma base de données en même temps »

Enfin, la procédure est terminée pour la création du compte et il ne vous reste plus qu'à attendre encore un jour pour que tout soit activé et opérationnel afin d'installer SWIR. Free vous parle alors de FTP. Nous allons voir dans le paragraphe suivant comment utiliser les paramètre que l'on vous donne.
J'ai choisi de vous faire découvrir free, mais il existe bien d'autres sociétés ou associations qui proposent un hébergement gratuit avec du PHP et du MySQL. Par exemple : http://web.ifrance.com avec de la pub ou http://www.multimania.lycos.fr/ encore avec de la pub. Vous pouvez trouver facilement des comparatifs sur le web, comme par exemple sur http://cyberzoide.developpez.com/php4/hebergeurs/

Installer SWIR

Si vous êtes arrivé ici, c'est que vous avez trouvé votre hébergement pour SWIR. Je vous rappelle qu'il faut pouvoir exécuter du PHP, que celui-ci supporte les sessions et avoir un base MySQL. Vous allez à présent décompresser l'archive zip ou tar.gz de SWIR dans un dossier de votre choix. Puis, il va falloir déposer tous ces fichiers sur le serveur de votre hébergeur. La manière la plus simple est d'utiliser une logiciel FTP (File Transfer Protocol), protocole de transfert de fichiers en français. Il en existe beaucoup, des gratuits comme des libres sur le Web. Pour les utilisateurs Windows, je conseille Filezilla, que vous pouvez trouver gratuitement sur http://filezilla.sourceforge.net/ et pour les linuxiens, gftp est bien sympathique.
Je vous explique succinctement l'utilisation d'un logiciel FTP sans entrer dans les détails car ce n'est pas le propos de cet article. Pour déposer des fichiers sur un serveur , il y a plusieurs solutions. Une très classique est d'utiliser le protocole FTP. Vous avez alors besoin de l'adresse FTP du serveur, d'un nom d'utilisateur et d'un mot de passe. Lancez votre logiciel FTP.
Vous trouvez généralement sur tous quelques champs à saisir en haut : l'adresse de votre serveur, pour free, c'est ftpperso.free.fr, le nom d'utilisateur et le mot de passe. Vous pouvez laissez le champ, port, vide pour utiliser celui par défaut (21). Quand vous cliquez sur l'icône de connexion, celle-ci

s'effectue en principe sans problème. Vous disposez souvent sur ce type de logiciels d'une partie centrale coupée en deux. La partie de gauche représente les fichiers locaux qui se trouve sur votre ordinateur, et la partie de droite les fichiers du serveur distant. Il faut alors que vous glissiez l'ensemble des fichiers contenus dans le dossier SWIR que vous avez décompressé, de la partie gauche vers la partie droite de votre logiciel FTP pour les uploader chez votre prestataire. Il faut bien prendre le contenu du dossier et non le dossier lui même. Il doit porter un nom du genre swir-0.2.6.2. Si tout ce passe bien, SWIR est en place au bout de quelques minutes suivant la vitesse de votre connexion. Avant de quitter votre logiciel FTP préféré, il vous reste encore un chose à faire si vous êtes chez free afin d'activer les sessions. Il faut créer un répertoire sessions à la racine de votre site. Pour cela, un clique droit dans la fenêtre représentant les fichiers distants, puis créer un nouveau dossier et le tour est joué.

Dernière phase de l'installation, il faut renseigner SWIR sur les identifiants vous permettant de vous connecter à votre base de données et définir deux utilisateurs. Pour ce faire, il vous suffit de vous connecter à l'adresse de votre site. Par exemple, pour moi c'est http://concours.swir.free.fr. La procédure d'enregistrement commence automatiquement. Dans un premier temps, SWIR vous demande d'accepter la licence GPL, puis de valider votre choix. Ensuite, vous passez à l'étape 1 qui permet d'entrer les renseignements pour accéder à votre base de données. Pour free, le serveur est sql.free.fr, le nom de la base de données est le même que le nom de votre compte en remplaçant le « . » par des « _ ». Pour moi, ça donne concours_swir. Le nom d'utilisateur est le nom du compte dans mon cas concours.swir et enfin le mot de passe est celui que vous avez donné lors de la création du compte. Pour ma part c'est ... oups ce truc là, il ne faut pas que je vous le donne.

Vous validez et passez à l'étape 2. SWIR vous propose alors la création de deux utilisateurs. Le premier aura tous les droits sur le site et le deuxième pourra gérer les pages et les menus mais ne pourra pas toucher à l'apparence du site. L'idée ici est qu'un utilisateur va définir une charte graphique pour le site et que l'autre ne pourra pas la modifier afin de limiter les élucubrations graphiques, que l'on peut trouver sur certains sites, et qui sont généralement horribles. Voilà, c'est fini, vous êtes à l'étape 3, qui est la dernière et qui vous demande si vous voulez vous rendre immédiatement sur votre nouveau site ou entrer dans la partie administration. Simple l'installation, non? Voyons à présent comment utiliser cet outil.

Travailler avec SWIR

Avant d'aller plus loin, je vous propose d'avoir une petite réflexion sur la conception d'un site Web. En effet, on pense généralement que la création d'un site se résume à une bonne maîtrise des outils techniques et que le reste va tout seul. Et bien c'est faux. En tout cas, c'est mon avis. Pour moi, la conception d'un bon site web consiste à surmonter trois difficultés de même poids. La première est l'organisation des informations. Celle-ci, demande une réflexion importante qui va faire que le visiteur va trouver rapidement ce qu'il cherche ou va se perdre dans le méandre de vos pages. C'est d'ailleurs une des parties du concours, organiser les rubriques de Net Secret's. Ensuite, il y a la partie graphique, qui, si dans un premier temps semble moins importante, sera des plus cruciale pour que l'internaute se plaise sur votre site et y reste ou y revienne. Enfin, reste la partie technique, et c'est à que SWIR peut vous être d'un grand secours car vous constaterez qu'il se prend rapidement en main. Bon, trêve de discours, entrons dans le vif du sujet. Toute l'administration de votre site va pouvoir se faire dans votre navigateur favori. Pour accéder aux pages d'administration, il faut vous identifier avec un des utilisateurs que vous avez créés à l'adresse : http://adresse_de_votre_site/admin.php.

Cette page peut prendre un peu de temps au chargement. Une fois identifié, faites le avec l'utilisateur qui a le plus de droits pour que nous soyons devant la même interface.

Passons aux deux premiers liens en haut.

Les menus et sous-menus

Comme je vous l'ai déjà dit, une chose très importante dans un site est l'organisation de l'information.

renseigner SWIR

C'est pour cette raison que SWIR limite volontairement la navigation à un menu principal, qui peut contenir jusqu'à 9 liens, et un sous-menu pouvant lui aussi contenir 9 liens et changer pour chaque lien du menu principal. Si vous cliquez sur « Editer menu principal », l'interface vous propose de définir le nom de vos 9 liens du menu principal, la page qui sera appelée pour chaque lien et le sous-menu qui devra apparaître. Si vous n'avez pas 9 liens dans votre menu principal, ce n'est pas grave, laissez les derniers champs en bas à gauche non remplis. De même, si vous ne souhaitez pas appeler un sous-menu pour un lien donné, choisissez 0 dans la liste déroulante. De la même façon, vous n'êtes pas obligé de définir immédiatement la page qui sera appelée par chaque lien car elle n'existe probablement pas encore. Cette phase est juste pour commencer à organiser votre pensée et la façon dont vous allez présenter l'information.

Une fois que vous avez défini votre menu principal et quels liens feront appel à un sous-menu, il faut renseigner les sous-menus en question. Pour cela cliquez sur « Editer sous-menu ». C'est le sous-menu n°1 qui est en édition par défaut. Si vous voulez en éditer un autre, il faut sélectionner son numéro dans la liste déroulante, puis valider. Vous en avez 10 à votre disposition. Ensuite le principe est le même que pour le menu principal. Il faut renseigner le nom du lien et la page appelée. Il vous faut surtout ne pas oublier de valider en bas de la page pour que les modifications soient prises en compte. Donc, pour résumer la situation : quand vous allez cliquer sur un lien du menu principal, cela aura pour effet de faire apparaître une page et éventuellement un sous-menu qui porte un certain numéro entre 1 et 10.

Une fois le menu principal et les sous-menus définis, vous avez déjà



page d'administration de SWIR.

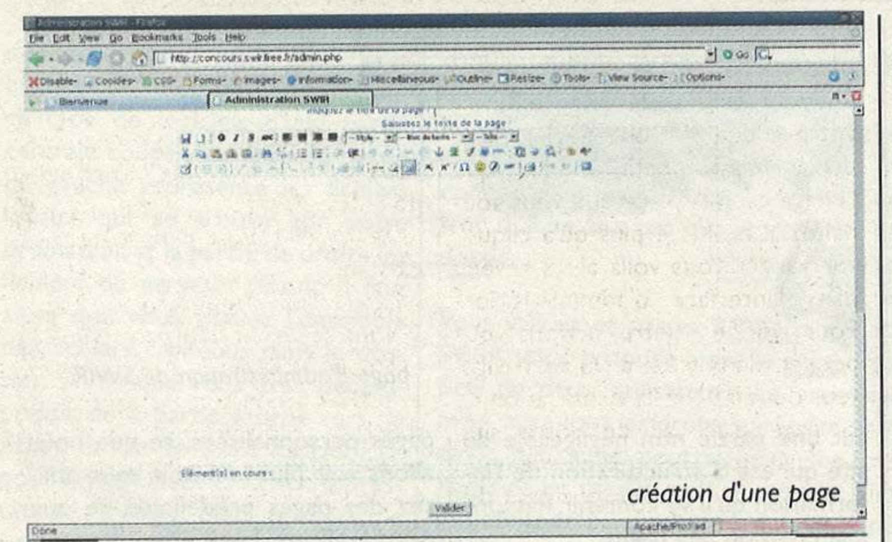
fait une partie non négligeable du site qui est la structuration de l'information qu'il va contenir. Passons à la création des pages.

Une petite remarque quand même avant de passer à la suite. Lors de la saisie de vos menus et sous-menus, SWIR vous a peut-être demandé de vous identifier à nouveau. C'est normal, car SWIR vous autorise à travailler une heure seulement. Ce système peut paraître contraignant mais permet de sécuriser un peu votre site. En effet, dans le cas ou vous oublieriez de quitter l'espace d'administration sur un ordinateur pouvant être utilisé par d'autres, la déconnexion se fera automatiquement dans l'heure. Vous pouvez remarquez que vous disposez d'une indication sous le titre « Administration ». Ce compteur vous renseigne sur le temps qu'il vous reste en secondes et est mise à jour chaque fois que vous cliquez sur un menu. Donc, si par exemple vous allez commencer la création d'une page assez complexe et qui risque de vous prendre du temps, je vous conseille de quitter et de vous identifier de nouveau pour disposer de l'heure entière. Sinon, pour les plus aguerris, vous pouvez toujours modifier cette durée en remplaçant les 3600 secondes indiquées à la ligne 129 du fichier identif.php.

Les pages prédéfinies

Enfin, nous arrivons à la création des pages. SWIR vous propose deux choses, soit vous créez des pages personnalisées, ce que nous allons voir plus loin, soit vous utilisez des pages prédéfinies, ce que nous allons voir maintenant. Cliquez sur « Créer / Modifier les pages ». L'interface vous demande si vous voulez éditer une page déjà existante et donc présente dans la liste déroulante de gauche ou créer une nouvelle page en saisissant son nom dans le champ de droite. C'est ce que nous allons faire. Mais attention, le nom d'une page doit respecter quelques règles. Premièrement, il ne doit pas dépasser 50 caractères. Ensuite, je vous conseille vivement de n'utiliser que des chiffres et des lettres non accentuées et éventuellement des « _ » ou des « - ». Donnez donc un nom à votre première page et cliquez sur « Modifier / Créer ». SWIR vous offre alors la possibilité de choisir entre 10 types de pages prédéfinies. Je pense que les petites miniatures sont suffisamment explicites. Vous voyez que vous avez le choix entre différents agencements de textes, d'images et de vidéos. Prenons un texte simple. Le premier en haut à gauche. Il est d'ailleurs sélectionné par défaut. Puis validez. Deux zones de saisie apparaissent. Une pour définir un titre à la page, mais ce n'est pas obligatoire, et une autre munie d'une barre d'outil type traitement de texte.

Vous pouvez alors saisir votre texte dans ce champ et le mettre en forme. Attention à ne pas trop abuser des


création d'une page

outils de mise en forme qui vous sont proposés, car il existe une autre solution moins souple mais plus rigoureuse que je vous expliquerai par la suite. J'en profite pour remercier les auteurs de cette magnifique barre d'outils, car elle n'est pas de moi, et vous pouvez trouver tous les renseignements que vous voulez sur celle-ci sur le site http://tinymce.moxiecode.com/ . Franchement c'est un travail remarquable qui a été réalisé et qui mérite d'être souligné. Je tire mon chapeau, blanc bien sur, aux auteurs. Une fois votre texte saisit et mis en forme, vous validez en bas. Vous avez alors un aperçu de ce que va donner votre page. Il faut à présent définir le lien qui va appeler celle-ci. Suivant que ce lien est dans le menu principal ou dans un sous-menu, éditez le menu ou sous-menu correspondant, puis dans la liste déroulante en face du lien, vous devez voir apparaître votre page. Vous la sélectionnez puis vous validez le menu en question. Pour contrôler la bonne affectation, c'est tout simple. Rendez vous sur votre site. Demandez l'actualisation de la page en cours, c'est généralement F5 sur les navigateurs. Cliquez sur le lien qui mène à votre page et celle-ci doit s'afficher à l'écran. C'est tout simple, non?

Allez, Faisons-nous une autre petite page pour bien comprendre le mécanisme. Je vous propose cette fois de prendre le premier type prédéfini de la deuxième ligne, celui qui propose une image avec du texte au-dessous. Même procédure que précédemment. Mais quand vous validez le type, vous vous rendez compte que les champs qui vous sont proposés reflètent la structure de la page que vous avez choisie. Le problème pour le moment, est que la liste déroulante proposant les images disponibles sur le serveur est vide. En effet, nous n'avons pas encore déposé d'images pour notre site. Si vous souhaitez le faire maintenant, je vous invite à lire la partie « La gestion des fichiers images, vidéos et documents » un peu plus loin. Une fois que quelques images sont déposées sur le serveur, vous allez les voir apparaître dans la liste. Vous pouvez alors finir votre page, puis l'associer à un lien comme précédemment. Et encore une page mise en ligne :-) .

Arrivé à ce stade, vous avez compris une bonne partie de la philosophie de SWIR et j'espère qu'elle vous plaît. Voyons ensemble les autres fonctions que vous propose ce CMS.

Les pages personnalisées

Comme je vous l'ai mentionné dans la création des pages prédéfinies, l'utilisation abusive des fonctionnalités de la barre d'outils des zones de texte conduit généralement à des problèmes de mise en forme du document et des incohérences graphiques. C'est pour cette raison que SWIR propose un type de pages personnalisées vous permettant de cadrer un peu l'information. Quand vous allez réaliser une page, il faut au préalable vous imaginer sa structure. Je mets du texte là, puis deux images ici... Le mieux est de se placer face à une feuille, puis de la découper en lignes et colonnes et de choisir ce que vous mettez dans chaque case. Une fois ce travail fait, vous pouvez définir facilement le nombre de tableaux ainsi que le nombre de lignes et de colonnes pour chacun d'eux. La page personnalisée est pratiquement faite. Dans l'interface de création de pages de SWIR, choisissez « Page personnalisée », puis définissez le nombre de tableaux qu'elle doit contenir. Validez. Donnez alors le nombre de lignes et de colonnes de chaque tableaux. Enfin, définissez le contenu de chaque case. Et voilà, il n'y a plus qu'à saisir le contenu de la page et valider. Je vous laisse faire vos essais.

Petites remarques importantes.

Si vous créez un page personnalisée qui porte exactement le même nom qu'une page prédéfinie, c'est la page prédéfinie qui est prépondérante.

La page « accueil », est une page particulière que SWIR affiche quand l'internaute arrive sur votre site. Il ne faut donc pas la supprimer, mais la modifier. De plus, si vous voulez que celle-ci soit une page personnalisée, il faut créer une page personnalisée portant le nom « accueil » et supprimer la page prédéfinie portant ce même nom dans la section « Gérer les pages ».

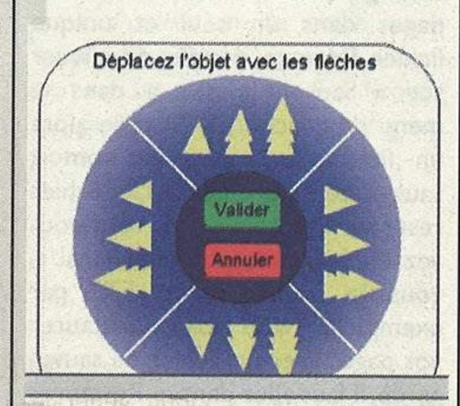
La gestion de l'apparence du site

Jusqu'à présent, nous avons créé des pages mais nous n'avons pas parlé de l'aspect graphique du site. Ceci à pu vous frustrer car généra-

lement on s'occupe de la partie graphique du site avant de construire les pages et de structurer les données. C'est à mon sens une erreur, car maintenant que vous savez exactement ce que vous voulez pour votre site, vous allez pourvoir lui appliquer un graphisme qui lui correspond parfaitement.
SWIR ne propose pas énormément de fonctions graphiques mais suffisamment pour avoir un joli design sans surcharger l'interface. Vous avez la possibilité de mettre une image de fond et deux autres images que vous pouvez placer sur la page comme bon vous semble. Vous pouvez aussi placer au pixel près, chaque lien du menu principal et du sous-menu. Toutes ces fonctions sont réunies dans la section « Gérer l'apparence du site ». Comme chaque partie de cette section est commentée dans SWIR, je ne vais pas m'étendre sur les choses simples, mais plus vous parler de quelques subtilités.
Le placement des images mobiles et des menus se fait d'une manière un peu particulière. Je vais vous donner un exemple avec la première image mobile, sachant que tous les positionnements d'objets sont basés sur le même principe. Dans la section « Gérer l'apparence du site », cliquez sur « Gérer la première image mobile », SWIR vous offre alors la possibilité de choisir cette image sur votre ordinateur, afin de l'uploader, ou de l'effacer, mais ce n'est pas notre propos pour le moment. Dans le texte, au-dessous du champ, vous avez un lien « Panneau de positionnement ». Cliquez dessus. SWIR calque alors l'interface d'administration sur le graphisme actuel de votre site et vous fait apparaître une roue de positionnement. Les flèches de celle-ci vous permettent de déplacer d'une petite, moyenne, ou grande distance l'image et ce, dans toutes les directions.

Attention, il arrive parfois d'avoir un petit temps de latence entre votre clique sur une flèche, et le déplacement effectif. Une fois que l'image est à la place que vous souhaitez, il ne reste plus qu'à cliquer sur valider. Vous voilà alors revenu dans l'interface d'administration. Pour vérifier votre action, vous pouvez demandez à votre navigateur de rafraîchir la visualisation de la page d'accueil de votre site. Le principe est exactement le même pour le positionnement des menus. Ce travail peu sembler un peu long au départ, mais il présente l'avantage de se faire directement dans le navigateur et donc où que vous soyez à partir du moment ou vous avez une connexion internet. De plus, on ne change pas la position des menus et des images d'un site tous les jours.

Une autre partie importante dans la gestion de l'apparence de votre site est celle de la cohérence graphique. Sans vouloir atteindre la précision des chartes graphiques des grandes entreprises, nous pouvons quand même faire un effort pour respecter une identité graphique et éviter le mélange de couleurs et de polices que nous pouvons voir sur certains sites. Pour ce faire, SWIR vous propose la création de styles de caractères. Rendez-vous dans la partie « Gérer l'apparence du site => Gérer les styles ».



Interface de positionnement des objets

SWIR vous propose alors trois possibilités :

- la modification du style des liens. Tous les liens auront le même style pour tout le site.
- La modification d'un style déjà existant.
- La création d'un nouveau style.

Si vous créez un nouveau style, par exemple « style_1 », là encore, évitez les accents et les caractères spéciaux ainsi que les espaces, vous pouvez définir une couleur, une police.. pour ce style. Par la suite, quand vous allez créer une page et que vous remplirez une zone de texte, vous allez pouvoir appliquer ce style à votre texte. Pour ce faire, éditez ou créez la page où se trouve le texte auquel vous voulez appliquer votre nouveau style. Sélectionnez le texte puis, dans le menu style de la barre d'outils, sélectionnez celui que vous voulez. Si le style que vous venez de créer n'apparaît pas encore, il faut demander une actualisation de la page d'administration. Le gros avantage est que si à présent vous modifiez ce style, tous les textes qui ont ce style, vont aussi être modifiés. Ceci permet de faire évoluer très rapidement la charte graphique d'un site.

La gestion des fichiers images, vidéos et documents

Lorsque vous avez installé SWIR, vous avez déposé les fichiers par FTP. Pour pouvoir disposer d'images, de vidéos et éventuellement de documents téléchargeables pour l'internaute, il faut que ces fichiers soient déposés sur le serveur de votre prestataire afin que vous puissiez en disposer pour la création de vos pages. Pour Uploader vos fichiers, vous pouvez aussi passer par FTP. Les images doivent être déposées dans le dossier « images », les vidéos dans « videos » et les documents, comme par exemple les fichiers PDF, dans « documents ».

créer des styles

Il peut néanmoins arriver que vous ne disposiez pas d'un logiciel FTP pour transférer vos fichiers sur le serveur. Par exemple si vous n'êtes pas sur votre ordinateur. Imaginons que vous soyez en déplacement et que vous veniez de prendre une photo avec votre appareil numérique. Vous souhaitez construire rapidement une page Web pour la montrer. Et bien, il vous faut juste trouver un ordinateur disposant d'une connexion internet. Vous déposez la photo sur le disque dur de celui-ci. Vous vous identifiez sur la page d'administration de votre site et vous allez dans « Gérer les images ». Vous visualisez alors la liste des images déjà disponibles sur le serveur. En bas de la page, vous trouvez un champ vous permettant de déposer une nouvelle image. Vous cliquez sur « Browse... » et vous allez chercher celle-ci sur la machine locale. Vous validez, l'image est uploadée et est immédiatement utilisable pour construire une nouvelle page.

Attention, il existe néanmoins quelques restrictions. Les fichiers images doivent être de type jpeg, gif ou png, et ne doivent pas dépasser la taille de 1Mo. SWIR n'intègre pas pour le moment un système permettant de modifier les dimensions d'une image. Donc, lorsque vous déposez une image sur le serveur, elle doit avoir été mise à la bonne taille. Je vous conseille de ne pas dépasser les 640x480 points. Généralement, une image de 320x240 points est déjà d'une bonne dimension pour une page web.

En ce qui concerne les vidéos et les documents, le principe est le même. Les vidéos doivent être de type mpeg ou avi et ne pas dépasser la taille de 5Mo. Pour les documents, faites attention car il n'y a pas de restriction de type et tout peut être déposé. Cette solution permet une grande souplesse mais au détriment de la sécurité. Alors soyez attentif sur qui a le droit de déposer des documents sur le serveur. Ceux-ci doivent avoir une taille maximale de 5Mo.
Voilà pour ce qui est de la gestion des fichiers sur le serveur. Je pense que les autres petites fonctions de cette partie sont suffisamment explicites et je ne rentrerai pas dans les détails, sinon cet article va finir par occuper tout le Net Secret's ;-).

Quelques fonctions bien sympathiques

Enfin nous arrivons au terme de cet article et, je pense qu'à ce stade seul, les plus courageux sont encore avec moi. Je vous en félicite. J'ai donc gardé les deux meilleures fonctions de SWIR pour la fin. SWIR vous donne la possibilité de sauvegarder l'ensemble de vos pages dans un seul et unique fichier. Pour ça, il suffit de cliquer sur « Sauver le site » dans le menu de gauche. SWIR crée alors un fichier qui porte le nom « sauv_date_heure.sql ». Ce fichier reste sur le serveur, mais vous pouvez en faire une copie en local si vous le souhaitez, via FTP par exemple. Si vous voulez restaurer vos pages avec un fichier de sauvegarde, il faut allez dans « Restaurer le site » puis cliquer sur « Restaurer le site avec ce fichier » en face de la sauvegarde qui vous intéresse. Attention, toutes les pages actuelles seront détruites et vous ne disposerez que des pages que vous aviez au moment de la sauvegarde choisie. C'est pour cette raison qu'il est prudent de toujours faire une sauvegarde avant une restauration.

Cette restauration ne concerne que les pages et non l'aspect graphique du site, quel dommage ;-) Mais non, SWIR propose aussi une sauvegarde de l'apparence de votre site, en gros toute sa charte graphique, y compris l'image de fond et les images mobiles sont sauvées, mais cette fois sans les pages. Il faut allez dans « Gérer l'apparence du site », puis dans « Sauvegarder le graphisme du site » et le tour est joué. Ceci vous permet de tester plusieurs styles graphiques pour votre site en les sauvegardant et en les restaurant à votre guise. Faites vos essais.

Conclusion

Résumer en quelques pages l'installation et le fonctionnement de SWIR n'est pas chose facile. J'espère ne pas avoir ennuyé les pros de l'informatique et avoir été suffisamment claire pour le néophytes. Je pense que SWIR est loin d'avoir fini son chemin, que beaucoup de choses sont encore à améliorer mais que c'est un début. Je compte sur vous pour me faire part de vos remarques. Qu'elles soient constructives ou non. J'ai déjà reçu quelques mails d'encouragement et ça fait toujours plaisir de voir que les heures que j'ai passé et que je passe encore sur ce système, peuvent servir à d'autres.
Je vous souhaite donc à toutes et tous bonne chance pour le concours et que le meilleur gagne.

CodeJ

Surfez avec TUX

Nous allons voir dans cet article comment configurer son réseau filaire sous Linux. Nous nous placerons dans un cas assez courant de configuration du réseau proche de bon nombre d'installations domestiques : une machine et un routeur lui-même relié à internet (soit directement soit par le biais d'un modem). La distribution Linux qui nous servira de support pour les illustrations sera une distribution Debian, la Debian GNU/Linux 3.1, alias sarge, pour être plus précis. Nous allons progresser par étapes, certaines ne concerneront que certains d'entre vous.

Étape 1 : prendre en compte le matériel

Avant même de se lancer dans la configuration de votre réseau filaire, il faut être sûr que votre carte réseau est bien prise en compte par votre noyau Linux. Pour cela, un lsmod vous permettra de voir les modules chargés (je n'ai repris qu'une partie) :

```
megalochelys:~# lsmod
Module                  Size  Used by
radeon                113956  2
lp                     10408  0
ipv6                  229892  23
usblp                  12032  0
...
eth1394                19976  0
sym53c8xx              69652  0
scsi_transport_spi     12160  1 sym53c8xx
via_rhine              19848  0
mii                     4864  1 via_rhine
ohci1394               32004  0
...
```

Dans mon cas, c'est le module via_rhine qui se charge de la gestion de ma carte réseau. Si vous ne voyez aucun module correspondant à votre carte réseau, c'est que soit la prise en charge est faite directement dans le noyau (est dans ce cas vous pouvez passer à l'étape suivante), soit que vous n'avez pas encore le module de chargé. L'objectif n'est pas ici de faire un descriptif du fonctionnement du noyau Linux. Les commandes lspci (permettant d'obtenir des informations sur le matériel pci et assimilé de votre machine) et modinfo (permettant d'obtenir des informations sur un module) devraient vous suffire en complément de votre moteur de recherche préféré pour trouver le bon module à charger. Une fois le bon module trouvé, il ne vous reste plus qu'à le charger par un insmod, modprobe ou tout autre utilitaire de gestion des modules du noyau comme modconf par exemple.

Étape 2 : Configurer les informations de bases du réseau

C'est la commande ifconfig qui permet de configurer une carte réseau. Il est impossible d'explorer ici toutes les possibilités que vous offre cette commande, pour cela, je vous renvoie à la page de man de ifconfig. Par contre, nous pouvons donner quelques exemples basiques d'utilisation de cette commande. Le premier exemple à donner est un simple appel à ifconfig qui permet d'obtenir des informations sur les interfaces réseau :

```
megalochelys:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:09:C3:AA:9A
          inet addr:192.168.2.150  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::211:9ff:fec3:aa9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2765 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:255467 (249.4 KiB)  TX bytes:757876 (740.1 KiB)
          Interrupt:209 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
            RX packets:2679
errors:0          dropped:0
overruns:0 frame:0
            TX packets:2679
errors:0          dropped:0
overruns:0 carrier:0
              collisions:0
txqueuelen:0
            RX bytes:693732
(677.4     KiB)          TX
bytes:693732        (677.4
KiB)egalochelys:~#
```

Pour positionner l'adresse IP de l'interface réseau eth0 (la première interface réseau), un simple :

```
megalochelys:~#   ifcon-
fig eth0 192.168.2.152
```

positionnera l'adresse IP de eth0 à 192.168.2.152.

Il est bien évident qu'il existe un moyen de pérenniser la configuration d'une interface réseau. Sur une distribution Debian, les informations de base concernant le réseau se trouvent dans le fichier /etc/network/interfaces. Regardons ce qui se trouve dans le mien :

```
megalochelys:~# more
/etc/network/interfaces
# This file describes
the network interfaces
available on your sys-
tem
# and how to activate
them. For more informa-
tion, see interfa-
ces(5).

# The loopback network
interface
auto lo
iface lo inet loopback

# The primary network
interface
auto eth0
iface eth0 inet static
address 192.168.2.150
netmask 255.255.255.0
broadcast 192.168.2.255
gateway 192.168.2.1
```



Les lignes commençant par # sont des lignes de commentaires. Nous retrouvons deux blocs dans ce fichier, le premier bloc concerne la boucle locale et le second la configuration de l'interface réseau eth0. L'interface loopback ou boucle locale permet à votre machine de s'envoyer des paquets réseau. Elle est indispensable au bon fonctionnement de votre machine. Intéressons nous plus aux lignes de la partie consacrée à l'interface eth0 :

- auto eth0 signifie que l'interface eth0 doit être configurée automatiquement au démarrage
- iface eth0 inet static signifie que l'interface eth0 est une interface d'un réseau TCP/IP et que son adresse est fixée statiquement. Pour configurer cette interface en lui attribuant une adresse dynamiquement, il suffit de remplacer static par dhcp. Dans ce cas les lignes qui suivent celle-ci sont à enlever et les étapes suivantes sont inutiles car c'est le serveur dhcp qui se chargera de donner les renseignements des serveurs de noms et des routes à suivre.
- address 192.168.2.150 attribue l'adresse IP 192.168.2.150 à votre interface eth0
- netmask 255.255.255.0 positionne le masque de sous réseau de votre interface. Ici le réseau est un réseau de classe C.
- broadcast 192.168.2.255 définit l'adresse à utiliser pour faire de la diffusion.
- gateway 192.168.2.1 permet de définir la passerelle, c'est à dire l'endroit où tous les paquets qui ne sont pas destinés à une machine du réseau local seront envoyés. Charge à cette passerelle de faire le travail d'acheminement.

Étape 3 : Configurer les serveurs de noms

L'étape 2 nous permet de configurer notre carte réseau, il reste encore à donner les informations nécessaires au dialogue avec les autres machines du réseau. La base

de tout dialogue est de savoir où s'adresser. Il va donc falloir configurer les serveurs de noms qui vont nous permettre de s'affranchir de ces adresses IP un peu barbares (et encore, je parle que d'IPV4 ;-). Cette configuration se fait dans le fichier /etc/resolv.conf :

```
megalochelys:~# more
/etc/resolv.conf
search
nameserver 192.168.2.1
```

La première ligne sert à spécifier dans quel domaine vous chercher une machine par défaut. Par exemple, supposons que vous soyez dans le domaine toto.com, spécifier search toto.com dans le resolv.conf va vous permettre d'adresser la machine titi.toto.com simplement en l'appelant titi. Cette configuration est optionnelle comme vous pouvez le constater. La seconde ligne spécifie le premier (et ici le seul, mais il peut y avoir plusieurs lignes commençant par nameserver) serveur de noms à utiliser. C'est à ce serveur que les requêtes DNS seront envoyées.

Il est également possible de mettre des correspondances entre adresse IP et nom de machine dans le fichier /etc/hosts. Dans le cas d'une requête nécessitant la résolution de nom, si dans le fichier /etc/nsswitch.conf se trouve la ligne :

```
hosts:          files
dns
```

le système va d'abord regarder dans le fichier /etc/hosts et si il ne trouve pas de correspondance, il interrogera ensuite le serveur DNS.

Étape 4 : Regarder si ça fonctionne

Comme nous venons de le voir, il n'est pas très difficile de configurer son réseau filaire si l'on est dans une situation « classique ». Reste à voir si cela fonctionne bien. La première des choses à vérifier est qu'il est possible de se pinguer soit-même :

```
megalochelys:~# ping
localhost -c 1
PING localhost.localdo-
main (127.0.0.1) 56(84)
bytes of data.
64 bytes from local-
host.localdomain
(127.0.0.1): icmp_seq=1
ttl=64 time=0.039 ms

--- localhost.localdo-
main ping statistics --
-
1 packets transmitted,
1 received, 0% packet
loss, time 0ms
rtt min/avg/max/mdev =
0.039/0.039/0.039/0.000
ms

Le paquet est bien
arrivé à destination,
donc pas de problème
jusque là. Il est donc
possible d'aller plus
loin, en pinguant une
machine distante cette
fois-ci :

megalochelys:~# ping
www.acissi.net -c 1
PING acissi.net
(213.186.33.2) 56(84)
bytes of data.
64 bytes from
acissi.net
(213.186.33.2):
icmp_seq=1 ttl=120
time=558 ms

--- acissi.net ping
statistics ---
1 packets transmitted,
1 received, 0% packet
loss, time 0ms
rtt min/avg/max/mdev =
558.288/558.288/558.288
/0.000 ms
```

Il reste une chose intéressante à explorer en cas de soucis, c'est le routage. Cette partie à été passée sous silence car, dans la configuration dans laquelle nous nous sommes placés, le plus souvent, vous n'aurez pas à intervenir. Si ce n'est pas le cas, je vous renvoie à la page de manuel de la commande route. Si vous voulez obtenir des informations pour voir par où passent vos paquets, la commande traceroute vous permet d'obtenir ces informations. L'extrait de la sortie de traceroute vers www.acissi.net nous montre que nous sortons bien de notre réseau (212.27.55.126 est un routeur extérieur à notre réseau local).

```
megalochelys:~# trace-
route www.acissi.net
traceroute to
acissi.net
(213.186.33.2), 30 hops
max, 38 byte packets
 1  . (192.168.2.1)
0.371 ms  0.388 ms
0.567 ms
 2  192.168.254.254
(192.168.254.254)
568.863 ms  567.996 ms
617.416 ms
 3  * bzn-6k-5-
v201.routers.proxad.net
(212.27.55.126)
801.642 ms *
 4  * * *
 5  * * *
 6  rdb-2-
6k.routers.ovh.net
(213.186.32.153)
679.602 ms  620.270 ms
670.928 ms
...
```

CONCLUSION :

Vous êtes maintenant capable de configurer votre connexion ou que vous soyez. Il ne vous reste plus apprendre à automatiser les configurations de vos diverses accés à internet. Alors, en route pour l'article suivant .

SyDoRe

LES SCRIPTS BA

Tout le monde vous le dira : utiliser Linux vous mènera à écrire des scripts. Ne serait-ce que pour renommer des fichiers en série ou pour disposer de programmes qui configurerons le réseau différemment, suivant l'endroit où vous vous trouvez. Nous allons voir ici les bases du scripting Linux.

Au commencement, le cheebong

Le cheebong, ce n'est pas un animal sauvage de linuxland. Il s'agit d'une instruction qui se trouve toujours en première ligne d'un script, et qui va définir avec quel interpréteur de commandes votre script sera lancé. En effet, chaque distribution Linux possède plusieurs de ces interpréteurs, parmi lesquels on compte bash, sh, csh, zsh, ksh .... Chacun d'eux peut avoir ses spécificités, et vous serez peut-être amenés à utiliser dans votre script une commande que bash connaît, mais que sh ne connaît pas. D'où l'utilité de pouvoir forcer l'utilisation de bash dans ce cas.

Le cheebong commence par les deux caractère « #! », suivit du chemin absolu de l'interpréteur. Voici quelques exemples:

```
#! /bin/bash
#! /bin/sh
#! /usr/bin/python
```

Respectivement, ces cheebongs commandent une exécution avec bash, sh et python. Vous pouvez également utiliser un interpréteur que vous aurez vous-même codé, mais si tel est le cas je ne crois pas que cet article vous soit réellement adressé.

Et maintenant, le script !

Comme je vous l'ai dit dans l'introduction, il va être intéressant, si vous disposez d'un ordinateur portable, de pouvoir appeler différents scripts qui configurerons votre réseau avec les paramètres qui vont bien, suivant que vous soyez à la maison, au bureau ou chez votre meilleur(e) ami(e) (g33kette powaa). Voici trois script simples qui vous permettrons de faire cela, que vous pouvez créer en tapant « nano reseau_lieu » ou « vi reseau_lieu » (nano et vi sont deux éditeurs de textes bien connus sous Linux):

```
#! /bin/bash
ifconfig eth0
192.168.0.1
route add default gw
192.168.0.254
echo "nameserver
212.27.54.252" >
/etc/resolv.conf
```

reseau_maison

```
#! /bin/bash
dhcpcd eth0 #au bou-
lot, c'est cool le
DHCP fait tout pour
moi
```

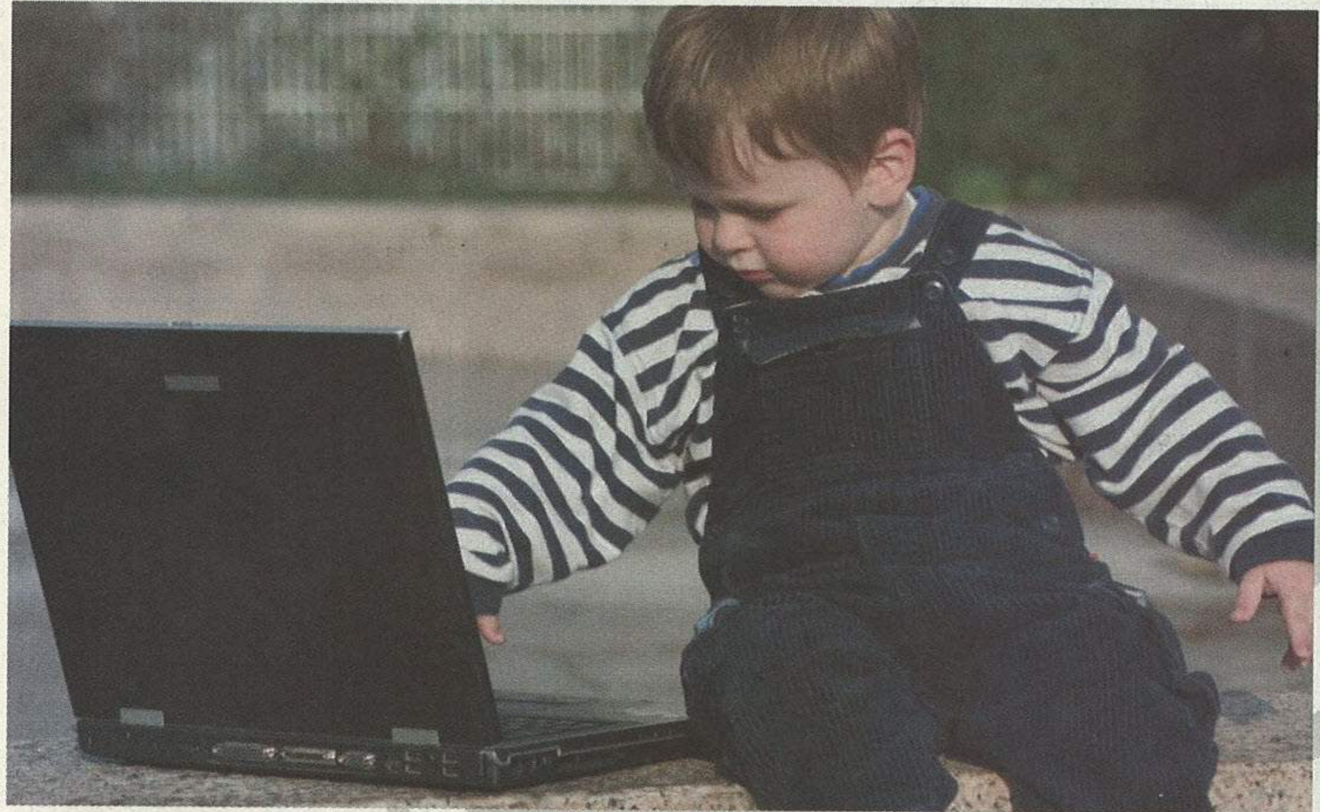
reseau_bureau

```
#! /bin/bash
ifconfig eth0
10.0.0.1
route add default gw
10.0.0.254
echo "nameserver
10.0.0.254" >
/etc/resolv.conf
#mon copain, c'est le
meilleur, il a même
un DNS chez lui !
```

reseau_bestfriend

Nous y configurons simplement une adresse IP, une route et une adresse de serveur DNS. Vous devrez adapter ces données a vos configurations personnelles, bien sûr. De même pour le réseau d'entreprise, vous n'utilisez peut-être pas la commande dhcpcd, mais une autre (dhclient ou pump, par exemple). Adaptez donc en conséquence. Ensuite, vous constaterez que j'ai inclus des commentaires, grâce au caractère # : il ordonne à l'interpréteur d'ignorer tout ce qui se trouve après lui sur la ligne. Je peux donc le placer indifféremment après une commande ou en début de ligne.

SH SOUS LINUX



Ces trois scripts, vous allez pour l'instant les enregistrer dans votre répertoire personnel (/home/votre_pseudo). Dans l'état actuel, si vous voulez les appeler, vous devez taper la commande « . reseau_lieu » (équivalente à la commande « source reseau_lieu », qui va interpréter le contenu du fichier comme si vous le tapiez au clavier).

La première étape va consister à rendre les scripts exécutables, c'est à dire qu'en tapant leur nom, ils se lancerons (sans avoir a mettre . ou source avant). Pour ce faire, tapez « chmod a+x reseau_* ». Cette commande va changer les attribut de tous les fichiers commençant par « reseau_ » (d'où le joker *) afin d'attribuer, à tout le monde (d'où le « a » devant « +x ») le droit en exécution sur les scripts (c'est l'utilité du « +x »). « man chmod » pour plus de renseignements.

Maintenant, pour lancer les scripts, vous pouvez taper ./reseau_lieu. Ce qui en fait ne change quasiment rien à la méthode précédente. En effet, le ./ sert à indiquer où se trouve le script (./ signifiant « le répertoire courant). Si vous voulez n'avoir qu'a taper le nom du script (de la même manière que vous tapez ls ou ifconfig), il vous faut placer ces script dans un répertoire connu du système. La liste de ces répertoires est indiquée dans la variable d'environnement PATH. Pour en connaître le contenu, tapez « echo $PATH ». Il ne vous reste qu'a placer vos scripts dans l'un de ces répertoire. J'utilise personnellement les répertoire /bin ou /usr/bin, de préférence. Mais, libre à vous d'en utiliser un autre. On pourrait également regrouper nos script dans un répertoire que nous ajouterions ensuite à PATH, mais ce n'est pas le but de cet article. Maintenant, tapez simplement le nom du script vous permet de le lancer.

Et de trois, la nature n'en fit plus qu'un

NET SECRET'S

```
#! /bin/bash

#Je vais récupérer quelques infos sur les
arguments

# $0 contient toujours le nom du script
SCR_NAME=$0

# $1 contient le premier argument, #2 le
second, et ainsi de suite
LIEU=$1

# $# contient le nombre d'argument passés en
paramètres
NB_ARGS=$#

# Si on n'a pas spécifié le LIEU ou
# Si on a mis trop d'arguments
# Un petit message indique comment s'utilise
le script
if [[ $NB_ARGS != 1 ]]
then
        echo "Usage : $SCR_NAME
{maison|bureau|bestfriend}"
else
        # Si on a passé "maison" en argument
        if [[ $LIEU = 'maison' ]] # attention
au espace autour des [[ et du =
        then
                ifconfig eth0 192.168.0.1
                route add default gw
192.168.0.254
                echo "nameserver
212.27.54.252" > /etc/resolv.conf
        fi

        # Si on a passé "bureau" en argument
        if [[ $LIEU = 'bureau' ]]
        then
                dhcpcd eth0
        fi

        # Si on a passé "bestfriend" en argu-
ment
        if [[ $LIEU = 'bestfriend' ]]
        then
                ifconfig eth0 10.0.0.1
                route add default gw
10.0.0.254
                echo "nameserver 10.0.0.254"
> /etc/resolv.conf
        fi
fi
```

Trois scripts, c'est bien. Mais si nous n'en n'avions qu'un que nous lancions avec un paramètre, ce serait mieux. Voici le script, commenté :

Les choses importantes à remarquer sont la syntaxe de la structure de test if .. then .. else.. (avec les doubles crochets pour les tests), ainsi que l'utilisation de variables.

La déclaration d'une variable se fait en donnant un nom à la variable (par exemple, SCR_NAME), et en lui affectant une valeur. Contrairement à d'autres langages, le script shell n'oblige pas de déclaration préalable. L'accès a la valeur de cette variable nécessite l'ajout du préfixe $ ($SCR_NAME).

Maintenant, en « chmodant » puis en déplaçant votre script comme vu précédemment, vous pouvez appeler « config_reseau maison », « config_reseau bureau » et « config_reseau bestfriend », et votre réseau est configuré en une commande. C'est toujours plus rapide que sur certains autres OS où ce genre de manipulation est inaccessibles pour 90% des gens, puisqu'il faut passer par une interface graphique ou créer des scripts grâce à un langage dont la documentation n'est pas toujours disponible.

Pour la suite, je pense que vous saurez faire des scripts plus complexes en regardant les scripts de démarrage. Vous rencontrerez des fonctions. Pour aborder ce concept, voici un exemple :

Dans ce petit script, je commence par décrire une fonction. Je lui donne simplement un nom (ma_fonction), que je termine par un couple de parenthèses pour préciser qu'il s'agit d'une fonction. Des crochets contiennent le code de ma fonction. Dans celle-ci, je

```
ma_fonction()
{
        if [[ $1 > 0 ]]
        then
                echo "Le nombre est supérieur
à 0"
        elif [[ $1 < 0 ]]
        then
                echo "Le nombre est inférieur
à 0"
        else
                echo "Le nombre est 0"
        fi
}

ma_fonction 12
ma_fonction -12
ma_fonction 0
```

Fonction

vais simplement effectuer des tests sur le premier paramètre de la fonction (remarquez que je ne fait aucun test sur la quantité de paramètres fournis, ce qui constitue une erreur), et afficher en conséquence sa position sur l'échelle des réels, par rapport à 0.
Une fois le corps de la fonction définie, je fait appel, par trois fois, a celle-ci, avec des paramètres qui vont me permettre de tester son bon comportement. Si tout se passe bien, vous devriez voire apparaître le résultat :

Le nombre est supérieur à 0
Le nombre est inférieur à 0
Le nombre est 0

Il faut bien faire attention car là encore, à l'inverse d'autres langages, les paramètres ne se passent pas entre parenthèses mais bien a la suite de la fonction, comme si nous invoquions une commande.
Vous trouverez aussi dans certains scripts les boucles FOR et WHILE. Ces boucles servent à itérer tant qu'un paramètre est et reste dans un état prédéfini. Voici un exemple très sommaire de ce que peuvent faire ces boucles :

Un script déjà un peu plus compliqué à lire quand on ne connaît pas bien. Première ligne, nous allons faire une boucle for que les programmeurs habituels ne connaissent pas forcément, mais qui est très utilisée : on va itérer sur une liste, celle des paramètres passés au script ($* représente cette liste). Le « do » désigne le début du corps du FOR, qui se termine par le « done », ligne 9. Ligne 3, on initialise j à 3. Puis, on itère grâce à une boucle while selon le prédicat « tant que j est supérieur à 0 ». « Supérieur à » se dit « greater than », en anglais; c'est la signification du « -gt », que l'on utilise, plutôt que les symboles > et <, en bash. Il existe -gt, -lt (less than, inférieur), -eq (equal), -ne (non-equal), -ge (greater or equal), -le (less or equal), et bien d'autres encore (man test pour plus d'informations).

Le « do » ligne 5 marque le début du corps du while. Ce while va écrire le paramètre actuellement traité par la boucle for (paramètre qui est donc contenu dans la variable i), puis décrémenter la variable j, ligne 7, pour éviter une boucle while infinie. Notez l'expression $((____)), qui signifie « évaluer ce qui se trouve entre le double couple de parenthèses »,donc la valeur de j ($j) moins 1, ce qui reviens à décrémenter J. Ligne 8, on permet au while soit de boucler, soit de se terminer. Pareil en ligne 9 avec le for.

Le résultat est l'affichage, 10 fois, de chaque paramètre passé au script.

Conclusion

Les commandes Linux commencent à n'avoir plus de secrets pour vous. Vous voilà maintenant capables de créer un script avec des fonctions, de tests et des boucles qui vous permettra de connecter votre ordinateur au réseau et de faire les montages réseaux adéquats. Les possibilités sont énormes et plus vous pratiquerez le « scripting » et plus vous en comprendrez les méandres. Alors à vos claviers...

KORETH

```
1  for i in $*
   2  do
   3          j=10
   4          while [[ j -gt 0 ]]
   5          do
   6                  echo $i
   7                  j=$(($j - 1))
   8          done
   9  done
```

for a while

Firefox, Qu'il est

Il existe actuellement un grand nombre de navigateurs internet. Vous pouvez trouver parfois des discutions très animées sur les forums pour dire que tel ou tel autre navigateur est le plus performant. Dans cet article je vous propose de vous faire découvrir non pas Firefox dans sa version de base, mais toutes les possibilités d'extensions qu'il offre à travers ses add-ons. Pour moi Firefox est l'un des meilleurs si ce n'est le meilleur que vous pouvez trouvez sur la toile.

Préambule

L'équipe de Net Secret's a décidé de vous faire découvrir non pas les fonctions classiques de ce navigateur que vous pouvez trouver généralement sur tous les autres mais les extensions possibles qui se comptent par centaines et je n'exagère pas. j'en ai parcouru pour vous plus de 400 et testé plus de 100. Je suis encore loin d'avoir tout exploré. Il est évident que nous ne pouvons vous les énumérer de façon exhaustive et nous avons donc fait une sélection pour vous. Cela va des fonctionnalités les plus futiles aux outils indispensables.

Chaque fois que vous installerez une extension il ne faudra pas oublier de redémarrer Firefox pour qu'elle soit prise en compte. Pour toutes les extensions dont nous allons parler, nous vous donnerons son nom. Cela vous permettra de la trouver facilement sur internet. Il vous suffira pour cela de vous rendre sur le site https://addons.mozilla.org et de taper dans la zone en haut à droite le nom de l'extension que vous recherchez puis de cliquer sur « Go ». Deux cas peuvent alors se présenter, soit l'extension apparaît seule sur la page et il ne vous reste pus qu'à cliquer sur « Install Now » pour l'installer, soit elle apparaît dans une liste parce que plusieurs add-ons existent pour le sujet recherché. Dans ce cas cliquez sur l'add-ons qui vous intéresse pour arriver sur sa page d'installation. Bon vous êtes prêt, alors en avant.

zoomer sur une image

Des fonctions pratiquement à l'infini

Voir les détails d'une images

Il arrive parfois qu'une image dans une page Web soit toute petite, ou que l'on souhaite voir un détail particulier. Avec « Image Zoom », Firefox vous offre la possibilité d'agrandir une image directement dans la page. Bien sur, si le zoom est important on voit apparaître les pixels de l'image, ce qui est parfaitement normal. Pour agrandir une image après l'installation de l'extension et redémarrage du navigateur, il vous suffit de vous placer sur l'image, puis un clique droit dessus et dans le menu contextuel vous voyez apparaître une nouvelle fonction « Zoomer sur l'image ». Choisissez alors le zoom que vous souhaitez et le tour est joué.

Une autre extension qui va bien aussi pour voir les détails d'une image est « zoomFox », mais cette fois l'agrandissement de fait dans un nouvel onglet de Firefox.

Des beaux onglets en couleur



: rusé ce renard

Vous savez certainement que Firefox permet la navigation par onglet. Ceci et très bien mais un peu de couleur dans ce monde tout gris ne fait pas de mal. Je vous conseille donc d'installer « Colorful Tabs » qui va mettre de belles couleurs sur vos onglets chaque fois que vous allez en demander un nouveau.

Visualiser tous ses onglets en un clin d'oeil

Nous venons de voir précédemment comment avoir de beaux onglets en couleurs. Mais si vous ouvrez plus de 5 onglets en même temps, il arrive généralement que vous ne sachiez ce qui se trouve sur chacun d'eux. Le titre de l'onglet est parfois insuffisant et vous les parcourrez tous un par un jusqu'à retrouver la page que vous cherchez. Ne serait-il pas plus facile de tous les voir en une fois. Et bien c'est possible avec « Showcase ». Après avoir installé l'extension et redémarré votre navigateur, ouvrez plusieurs onglets et chargez une page différente dans chaque. Puis, appuyez sur F12. Elle est pas belle la vie.

Vous pouvez vous rendre directement sur un onglet en cliquant dans son image, ou en fermer un en cliquant dans la croix en haut à droite de sa représentation.

Des jolies icons dans tous les menus

La encore ce n'est pas une extension indispensable, mais elle permet de rendre un peu plus agréable

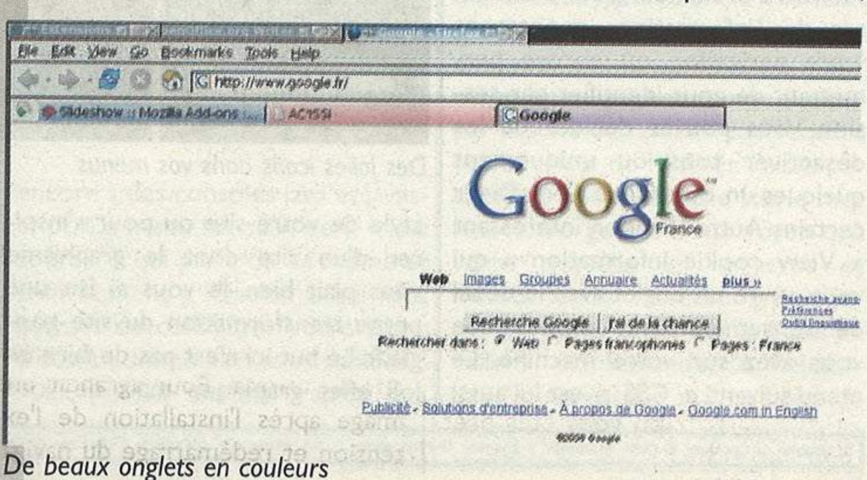


que Google est grand.

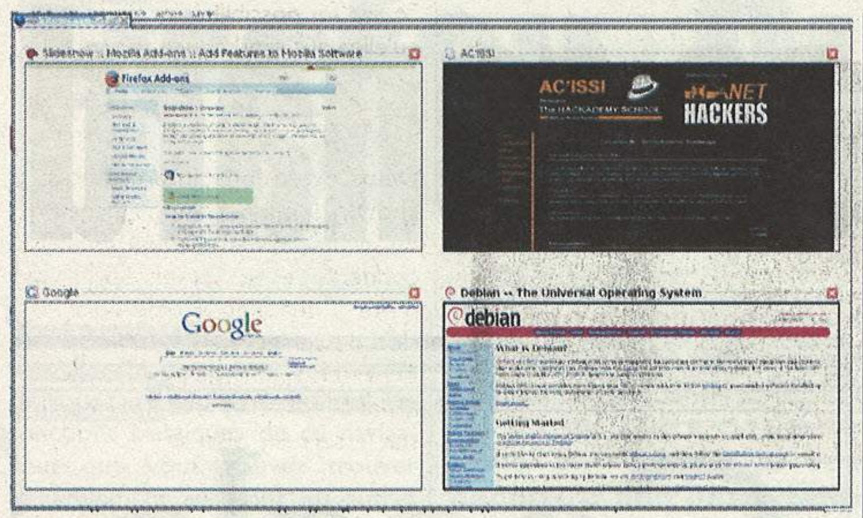
les menus souvent austères en y ajoutant plein de petites icons. Installez « CuteMenus – Crystal SVG » et jugez par vous même.

Analyser une page Web de A à Z

Jusqu'à présent je vous ai présenté des extensions permettant une amélioration de l'ergonomie et du graphisme de Firefox, mais nous allons à présent passer aux choses sérieuses et voir ensemble des extensions très utiles. La première que je vous propose est une barre d'outils que je considère indispensable pour décortiquer la façon dont est conçu une page Web. Cet ensemble de fonctionnalités pourra vous servir aussi bien pour comprendre comment une page à été conçue sur un site que vous visitez,



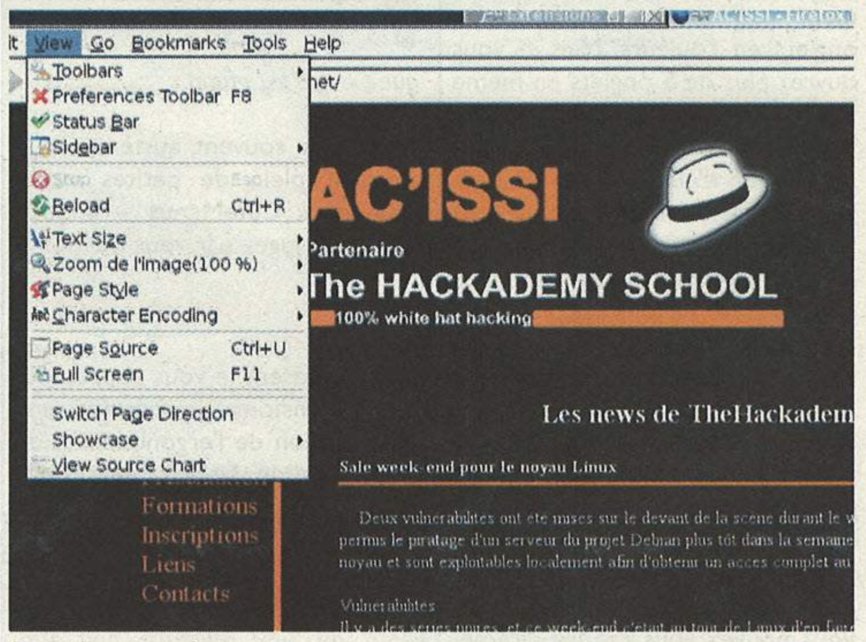
De beaux onglets en couleurs



Tous ses onglets en un clin d'oeil.

que pour vous aider à la conception du vos pages. Vous pourrez ainsi mieux cerner certains problèmes. Cette barre d'outils porte bien son nom puisqu'elle se nomme « Web developer ». Une fois installé, vous pouvez choisir de la faire apparaître ou non grâce au menu « View => toolsbar » ou « Afficheg => Barres d'outils ».

Nous allons à présent parcourir les menus de gauche à droite. Le premier, « Disable » vous donne la possibilité de désactiver certaine fonction de votre navigateur, comme le Javascript, ou certains éléments de la page comme la couleur. Le deuxième menu vous permet de travailler sur les Cookies. Ce sont ces petits fichiers déposés sur votre ordinateur pour mémoriser des informations concernant votre navigation ou encore permettant de vous identifier par session. Vous pouvez décider de les désactiver tous ou uniquement quelques un, ou encore d'en effacer certains. Autre fonction intéressant « View cookie information » qui vous ouvre un onglet avec le détail de l'ensemble des cookies que vous avez sur votre machine. Le menu suivant, « CSS », est lui aussi très utile. Il vous permet de visualiser, de désactiver et même d'éditer la CSS (Cascading Style Sheet ou feuilles de style en cascade) de la page que vous visualisez. Très sympathique pour affiner la feuille de



Des jolies icons dans vos menus

style de votre site ou pour s'inspirer d'un site dont le graphisme vous plait bien. Je vous ai fait une petite transformation du site google.fr. Le but ici n'est pas de faire un joli effet graphique mais de vous montrer les possibilité de cette extension.

Poursuivons avec le menu suivant qui concerne les formulaires « Forms ». Vous pouvez faire apparaître des informations sur les champs avec « Display forms Details », ou encore obtenir des données détaillées sur l'ensemble du formulaire avec « View Form Information ». Vous pouvez aussi visualiser les champs de mots de passe en claire, et encore bien d'autre chose. Je ne peut ici vous détailler toutes les fonctions de tous les menus car ce serait trop long et vous montre uniquement les fonctions qui me semblent les plus démonstratives.
Je pense que vous commencez à comprendre la philosophie de ces outils. Je vais donc allez un peu plus vite et vous laisser découvrir par vous même toutes les fonctions que vous propose Web Developer. Le menu « Images » permet d'obtenir toutes les informations possibles et imaginables sur les images

Disable• Cookies• CSS• Forms• Images• Information• Miscellaneous• Outline• Resize• Tools• View Source• Options•

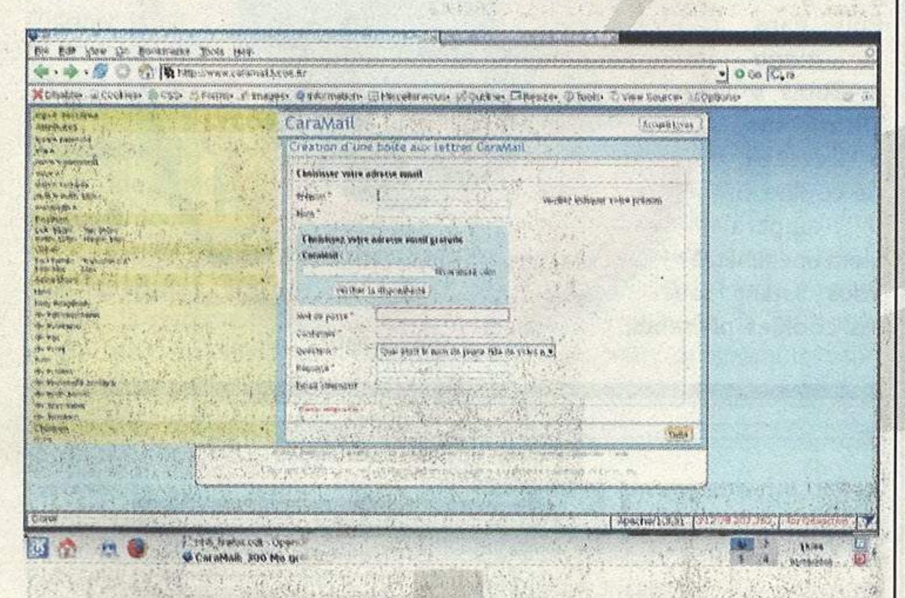
Une super barre d'outils



Qu'il est étrange ce Google.

présentes dans la page. Le menu « Information » permet quand à lui d'afficher une multitude de renseignements sur la page ou un élément de cette page comme par exemple « Display Element Information ».

» qui arrive. Il permet d'encadrer tout type d'élément dans une page. Utile pour voir la structure d'un tableau par exemple. C'est à présent au tour du menu « Tools » qui propose d'accéder directeur aux outils de validation W3C ou



Afficher les information d'un objet d'une page Web

Vous allez voir, ce n'est que du bonheur. Nous passons ensuite au menu « Miscellaneous » qui rassemble quelques outils inclassable. Comme par exemple des outils d'aide au positionnement ou encore l'édition du code html de la page. Puis c'est le menu « Outline

encore à des consoles java et javascript. Ce menu est suivi de « View source » qui parle de lui même et enfin le menu « Option » qui vous permet de configurer votre barre d'outils comme bon vous semble. Voilà, j'ai fait un tour rapide des fonctions que vous pouvez trouver dans cette super barre d'outils.

Testez ses possibilités et vous verrez qu'elle vous rendra bien des services.

Obtenir des informations sur le serveur distant.

Deux extensions intéressantes. « ShowIp » qui permet d'afficher l'IP du serveur distant auquel vous êtes connecté et « Server Spy » qui tente d'identifier le type et la version de ce serveur.
illustration : showip.png
légende : Afficher des informations sur le serveur distant

Modifier la requête HTTP (Hypertext Transfer Protocol)

Quand vous envoyez un requête à un serveur distant, que ce soit en GET ou en POST cet outil va vous permettre de modifier les données de la requête avant transmission. Installez « Tamper Data ». Vous trouvez alors en bas de votre menu Outils ou Tools la fonction « Altérer données ». Cliquez dessus. Vous avez une fenêtre Tamper data qui s'ouvre. Avant d'effectuer une requête sur une page ou de valider un formulaire, par exemple, cliquez sur « Démarrer l'altération » puis lancez votre requête dans Firefox. Vous constatez qu'à chaque envoie d'informations au serveur distant, Tamper data vous demande si vous vous voulez envoyer les données sans les modifier, ou si au contraire vous souhaitez les altérer. Si vous ne décidez pas pour le moment d'altérer les données, elles sont envoyées et mémorisées normalement. Vous pouvez alors décider par la suite de rejouer une requête et cette fois de l'altérer. Faites par exemple une recherche sur le mot linux dans google. Vous voyez que votre requête est envoyée et mémorisée sans altération. Puis faites un clique droit sur la ligne de celle-ci et demandez « Rejouer dans le navigateur ». Une boite de dialogue s'affiche et vous permet de modifier les données du formulaire.

Altérer les données d'une requête

Modifiez Linux en Windows puis faites ok et demandez de l'envoyer. Vous constatez que votre recherche n'est plus faites sur Linux mais sur Windows. Cette technique peut être très utile pour modifier certain champ qu'on ne voit par forcément, comme par exemple les champs cachés d'un formulaire.

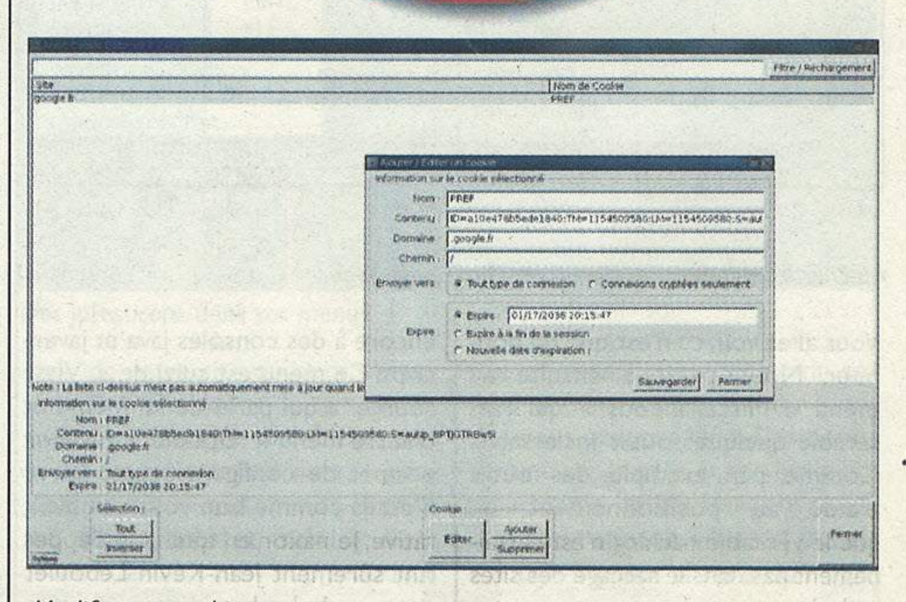
Éditer les cookies

Comme nous en avons déjà parlé, les cookies sont des petits fichiers que le serveur dépose sur votre machine et qui permet de le renseigner sur l'historique de votre navigation. Il peut par exemple indiquer que vous des droits d'administration ou que vous avez accès à des page réservées ou encore bien d'autres choses. Il peut donc être très intéressant de modifier le contenu d'un cookie pour tester la réaction du serveur et éventuellement palier à des failles de sécurité. L'outil que je vous propose est « Add N Edit Cookies ». Une fois installé, il va vous permettre de visualiser mais aussi d'éditer tous les cookies présents sur votre machine. Pour que la démonstration soit plus claire, je vous propose dans un premier temps de les effacer tous. Pour ça allez dans « Préférences » du menu « Édition » et dans la partie « vie privée » cliquez sur «Supprimer les cookies ». Ensuite allez sur la page google. Puis, dans le menu « Outils » allez sur « Éditeur de cookie ». Il apparaît alors une fenêtre vous listant tous les cookies présents, vous devez normalement n'en avoir qu'un. Vous pouvez alors cliquer sur « Éditer » afin de modifier les données de celui-ci.

Conclusion

Nous avons tenté de vous faire découvrir une face de Firefox que sont les extensions. Vous avez certainement constaté que le sujet est extrêmement vaste et nous ne pouvons que vous recommandez de faire vos propres découvertes. Vous remarquerez qu'il existe des fonctions vraiment utiles et d'autres beaucoup moins. Faites vos essais, car il est aussi facile d'installer une extension que de la supprimer en vous rendant dans « Extensions » du menu « Outils ». Alors à vos claviers.

CodeJ



Modifier ses cookies

Le dictionnaire du hacker

web : http://www.linux-france.org/prj/jargonf/ind/A.html

Sur le chat , on rencontre souvent des termes que l'on ne comprend pas toujours. Par peur du ridicule, on n'ose pas demander la traduction du terme et l'on ne comprend donc pas la phrase. La chose va être réglée, voici quelques termes souvent rencontrés.

1337 (leet) : Version abrégée de « eleete », déformation de « élite ». Pirate qui croit s'y connaître et s'imagine faire partie de l'élite des s... Le terme est péjoratif, sauf s'il est utilisé dans un contexte d'auto dérision.

geek : Fou, taré d'informatique, tout comme le . Typiquement, il est binoclard, avec des boutons, et théoriquement, sans petite copine (il ne sait d'ailleurs pas exactement ce que ça peut bien être).

hacker : À l'origine, programmeur de génie, terme parfois employé pour bidouilleur. Le terme de « Hacker » a perdu son prestige depuis le Crackdown de 1990, lorsque le système téléphonique US a globalement disjoncté, du fait d'une erreur de programmation des opérateurs, qui accusèrent pourtant le monde des BBS. Désormais, et surtout du fait des journalistes, le terme désigne surtout les pirates des réseaux. Voir aussi cracker.

hacktiviste : hacker mettant son talent au service de ses convictions politiques, et organisant des opérations coup de poing technologique : piratages, détournements de serveurs, remplacement de homepages par des tracts... Le terme devrait plutôt être « Cracktiviste », puisque le véritable hacking n'est certainement pas dans le saccage des sites web des autres.

h4x0r (haxor) : en remplacement du terme hacker

hoax : « canular » en anglais. Message destiné à se moquer de ceux qui le reçoive en les manipulant, en les poussant à répandre une rumeur, comme par exemple une fausse alerte de sécurité (alerte pouvant être totalement délirante, en particulier celles concernant les virus)

JAPH : Expression utilisée à l'origine par Randal L. Schwartz pour désigner un bidouilleur talentueux en Perl, et s'étant rapidement popularisée. On rencontre aussi la version développée « Just Another Perl Hack » pour parler non plus de la personne mais d'un petit programme utile, ou intéressant, ou remarquablement idiot.

lamer : Un minable, un nul, un crétin (« lame » signifie littéralement « boîteux », « estropié »), quelqu'un incapable de programmer son ordinateur pour mettre « bonjour » à l'écran, mais qui se prend quand même pour un hacker.

naxor : Un hacker qui devient « un nacker », puis « un naxor ». C'est une déformation plutôt péjorative, le naxor en question s'appelant sûrement Jean-Kévin Leboulet ou steve le hacker.

nerd : Taré, fou, fanatique qui passe ses journées devant un ordinateur, souvent sur le Net, et compte bien créer son propre serveur dès qu'il en aura les moyens

newbie : Contraction de « new in business ». Quelqu'un de nouveau, sur le réseau. On rencontre aussi « newcomer ». Un nouveau-venu, quoi... Qui ne sait rien et fait toutes les erreurs possibles et imaginables

noob : Déformation de newbie. Péjoratif.

r3b3l : Un « rebelle », qui ne se laisse par faire du tout. C'est probablement un hacker de renommée internationale dans son quartier.

roxer : De « to rock » en anglais, donnant « it rocks » une fois conjugué. Verbe utilisé pour désigner quelque chose de vraiment bien. Exemple : .

script kiddy : Petit morveux tout juste capable de faire tourner une poignée de scripts pouvant lui donner un accès non autorisé à un système, sans comprendre ce qui se passe réellement, mais se vantant d'être un vrai hacker. Il a tendance à être bête et méchant, et, est de ce fait relativement dangereux.

troll : un sujet qui fâche (ex: Mac ou PC ? perl ou python ? ...) , soit un individu qui persiste à lancer des discussions sur des sujets qui fâchent.

FaSm

Xbox 360 ou PSP, il y a touj pour profiter à fonds de sa

INTRODUCTION

Microsoft au lancement de la xbox 360 clamait haut et fort que leur console ne pourrait pas être hacké avant au moins deux ans… Mais c'était sans compter sur l'ingéniosité de certains bidouilleurs….

C'est au niveau du lecteur DVD que tout se passe, en modifiant le firmware (bios) du lecteur, il va être possible de lancer des copies de sauvegarde de jeux xbox 360. Sony ne cesse de sortir de nouveaux firmwares pour sa PSP et pourtant à chaque fois un hacker trouve une faille, découvrez les dernières possibilités pour la xbox 360 et la PSP.

Tout d'abord je vous rappel que vous devez procéder les originaux des copies de jeux que vous allez utiliser, dans le cas contraire, vous encourez de fortes amendes et peine de prison. Le but de cet article n'est pas de promouvoir le piratage de jeux, mais d'exploiter au maximum ses consoles de jeux vidéos.

I/ La xbox 360 hackée pour de bon !

1/ Flashage du lecteur DVD

Le 14 mai 2006, le premier firmware pour lecteur DVD est diffusé sur le net, son nom : Xtreme firmware. Dans un premier temps, ça ne fonctionne que sur le lecteur Samsung.

A) Détails techniques de l'Xtreme firmware :

- Lecture de la protection xbox 360 du secteur PSN 04FB1F (Layer 0)
- Lecture de la protection xbox 1 du secteur PSN 605FF (Layer 0)
- Le secteur protégé doit être extrait en utilisant Xtreme0800 360 firmware pour les jeux xbox 360 et xbox 1
- Ne peut pas lancer les copies de sauvegarde réalisée avec Xbox1 605b 0800 firmware

B) Méthode de flashage :

Pour flasher le lecteur, ce n'était pas chose simple, il fallait se fabriquer un PCB (une connectique pour relier le lecteur au pc), puis à l'aide du programme Key Drive Patcher/Xtractor v1.5, récupérer la clef du lecteur DVD pour les réintroduire dans le fichier xtrem.bin. Cette méthode ne fonctionnait pas sous Windows XP ou sous Linux, il fallait avoir un Windows 98 ?

Comme vous l'avez compris, ce n'était pas vraiment simple et en plus de ça, pas sure à 100 % car il y a eu pas mal de xbox 360 HS suite à cette technique.

Puis un firmware hacké pour le lecteur Hitachi / LG première version va également sortir, puis pour toutes les versions. Pour simplifier le flashage des lecteurs DVD, la Team Xecuter développa le Connectivity Kit. Cet adaptateur permet de relier le lecteur DVD à une prise SATA du PC et également à connecter le disque dur de la xbox 360 sur son PC toujours à l'aide d'une prise SATA.

C) Flashage avec le Connectivity Kit :

L'apparition du Connectivity Kit va permettre de flasher plus simplement son lecteur… On branche le lecteur DVD que l'on a retiré de la xbox 360 [voir photo branchement-lecteur-pour-flashage.jpg], on allume son ordinateur et on lance une commande DOS sous Windows XP, on se met dans le bon dossier et on lance le fichier .bat afin de flasher le lecteur [voir photo flashage-hitachi-01]. Des fichiers vont se créer dans ce dossier, il ne faudra pas les perdre car ils vous seront utiles si un jour vous voulez restaurer le bios d'origine de votre lecteur (pour mettre une puce dans la xbox 360 par exemple). Au moment où j'écris cet article, il est encore possible de jouer sur le xbox live avec le lecteur flashé, mais on ne sait pas si ça sera possible longtemps…

2 / Mettre une puce dans sa xbox 360

A force de voir apparaître des pseudos puces qui ne seront jamais vendues, il fallait bien qu'enfin il y en ait de commercialisées… C'est donc à partir du mois de juillet 2006 que les premières puces xbox 360 furent en vente. Ces puces sont à souder au niveau de la carte mère du lecteur DVD et évitent d'avoir à flasher celui-ci. Pour ceux qui avaient flashé leur lecteur, il suffit de restaurer le firmware avant de mettre la puce.

...ours une faille à exploiter ... console...

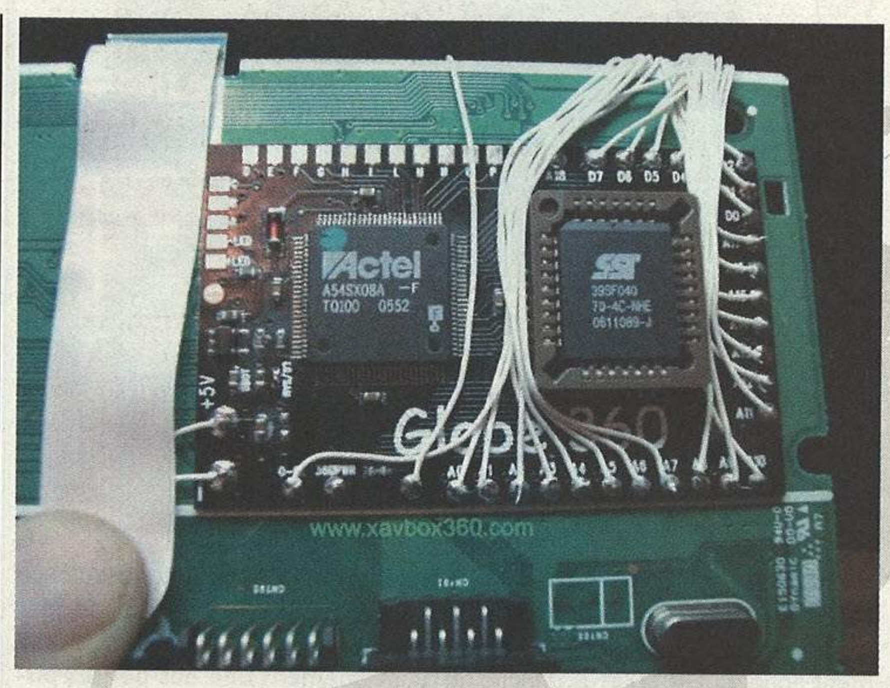
Au moment où j'écris cet article, deux puces ont vue le jour : la NME 360 et la Globe 360.

A) La NME 360

Développé par la Team Underdog (www.team-underdog.com) c'est la plus simple à souder des deux puces : 4 fils seulement si vous avez un lecteur Samsung et 11 fils si vous avez le lecteur Hitachi [3 photos au choix : commençant par « nme »]. En plus d'avoir plus de fils à souder pour l'Hitachi, il y a également la possibilité de régler le laser du bloc optique pour obtenir une compatibilité des médias insérés [une des 2 photos du « réglage Hitachi »]. Pour l'instant la méthode pour graver les DVD double couche pour cette puce est assez compliqué mais de nouveaux outils devraient sortir rapidement. Les copies de jeux qui fonctionnaient avec les lecteurs flashées ne fonctionneront plus, il faut graver différemment (tout simplement car la Team Underdog avait commencé à développé lorsque l'Xtrem bios et à mis les « security sectors » à une autre place). La puce détecte automatiquement si vous mettez un original ou une copie, ce qui permet de garder son Xbox Live intacte...

B) La Globe 360 :

Développé par la Team Globe (www.globe-360.com), cette puce est plus délicate à soudée car il y a plus de fils et surtout à souder à des points très petits... [voir photo globe-sur-hitachi-9.jpg]. Une trentaine de fils à souder et une piste à



couper, que ce soit pour le lecteur Hitachi ou le Samsung. La puce reconnaître automatiquement si vous avez mis une copie ou un original afin de booter sur le bon firmware (aucun soucis pour le xbox live). Le même système que l' Xtreme bios est utilisé, donc les backups sont les même que pour ceux qui avaient flashés leur console. La puce peut-être mis à jour si vous possédez un programmateur...

C) Autres puces pour xbox 360

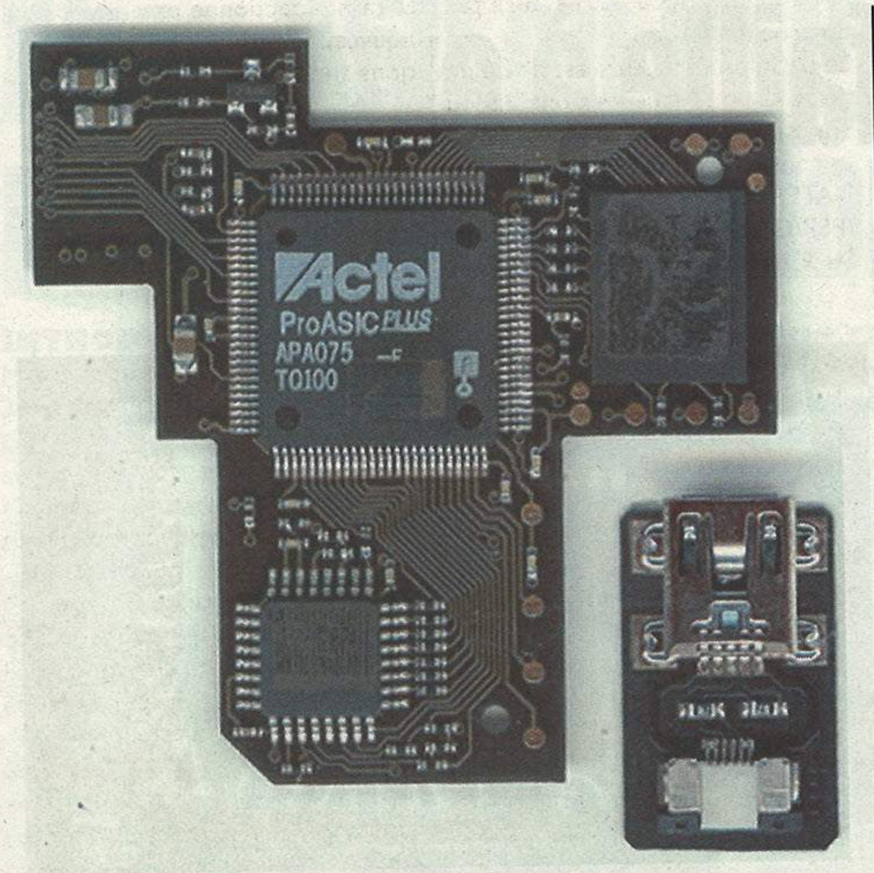
D'ici à la parution de l'article, il y aura sans doute de nouvelles puces de sorties, notamment la Fractal 360 (www.fractalteam.com) qui devrait être une bonne qualité...

La Xbox étant hackée depuis assez peu de temps, les possibilités évolues de semaines en semaines, alors pour pouvoir être certains de tout savoir et avoir des précisions sur ce que vous venez de lire, rendez-vous sur www.xavbox360.com

II / Toutes les PSP peuvent également être hackées !

Dans Net Secret's n°4 je vous disais qu'au dessus du firmware 2.0 on ne pouvait pas faire grand-chose, et bien les choses évoluent, maintenant on peut ;-)
Dark Alex (un membre plutôt actif de la scène PSP), avec l'aide de Mathieulh et Yoshiro à réussi à trouver comment downdgrader (action de redescendre de version le bios de la psp) un firmware 2.5 ou un 2.6 en 1.5 ! Pour ceux qui ont le firmware 2.7 ils peuvent mettre une puce dans leur PSP pour pouvoir lancer des homebrews et copies de jeux...

NET SECRET'S



A) Undiluted Platinum : la puce pour PSP [voir photo

La puce Undiluted Platinum, également appelée UP est très difficile à installer, même les soudeurs les plus expérimenter ont du mal, tant les soudures à faire sont minuscules…

La puce UP fonctionne sur tout les firmwares (donc pas de soucis pour le 2.7), elle ne nécessite pas de firmware hacké et lance tout les homebrews (softs développés maison) et copies de jeux. La puce est flashable avec le bios Epsilon à l'aide d'un soft et du câble USB fournit avec la puce.

Pour que vous puissiez vous rendre compte de la taille des soudure (sur une largeur de 8 mn il faudra souder 8 fils l'un à côté de l'autre), nous avons pris une photo la puce soudée à côté d'une pièce de un centime d'Euro [voir photo undileted-platinum-6 ou 7 ou 9]. Le montage de cette puce requiert un extrême habilité dans les soudures, une bonne vue, une grosse loupe ou mieux un microscope et un fer à souder avec une petite panne. Notez qu'il y a également une des petites pistes à couper…

Cette puce n'est pas vendue en France pour le moment et ne le sera peut-être jamais, mais quelle importance me direz-vous car peu de personnes sont capable d'un tel exploit pour souder (surtout que ceux qui ont réussi la pose d'une puce, ne vont pas forcément réussir la pose sur la PSP suivante…). Vous vous sentez capable de la souder vous-même ou allez faire appel à un technicien pour la poser, alors félicitation, vous allez avoir entre les mains une merveille technologique qu'il faudra apprivoiser pour flasher et la dompter…

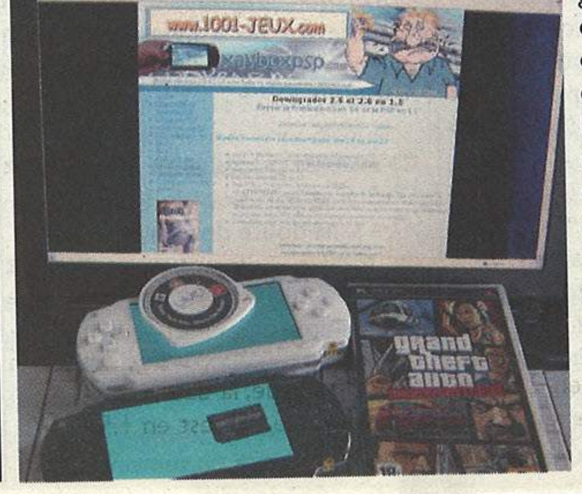
La puce peut s'activer ou non si on le désire. Quelle joie d'avoir une PSP avec un firmware 2.7 qui peut lire les copies de sauvegarde de jeux !

B) Downgrader 2.5 ou 2.6 vers 1.5

Le tant attendu Downgrader pour les versions 2.6 et inférieur est enfin apparut au mois de juillet (comme un cadeau de vacances pour certains).

Matériel nécessaire pour downgrader.

- Psp 1.5 pour réccupérer certains fichiers du nom de « downdater »
- Le firmware 1.5 (EBOOT .PBP)
- Memorystick pour mettre les fichiers
- PSP avec firmware 2.5 ou 2.6 (pour ceux qui ont la version 2.01, mettez à jour)
- UMD de GTA (Grand Thief Auto LibertyCityStories), la version ayant la faille…
- Downgrader_pack_final de Dark Alex



ATTENTION : le fait de downgrader agit sur le bios de votre PSP, en cas d'erreur votre psp peut devenir irrécupérable ! En suivant les tutos et en utilisant des fichiers saint (c'est-à-dire, pas des packs téléchargé par le biais du Peer To Peer, mais des fichiers que vous avez eu sur des sites sérieux traitant de la PSP, il ne devrait pas y avoir de soucis).

a) Le Downdater

Il va falloir trouver un copain/copine qui à une PSP 1.5 afin de pouvoir récupérer certains fichiers qui étant sous copyright ne se trouvent pas sur les sites PSP (prudence avec les fichiers que vous trouveriez sur des sources douteuses), cette manœuvre est sans aucun danger pour la psp de votre ami(e).

Prenez le pack de Dark Alex et copiez le contenu du dossier /1.50 HELPER/ dans /PSP/GAME/ (downhelper et downhelper%)
Ensuite créez un dossier /UPDATE/ (en lettres Majuscules) dans /PSP/GAME/ et placez y le firmware 1.5 (EBOOT.PBP).
Allumez votre PSP, puis rendez-vous dans "Jeux" et lancez le "downdater helper".
Au bout de trente secondes à une minute, après avoir vue défiler un paquet de texte, la PSP retourne au menu de démarrage et un dossier au nom de /DOWNDATER/ s'est créé à la racine du Memory Stick (c'est ce fichier qu'il faudra utiliser)

b) Le Downgrader

Le Jeux GTA possède une faille exploitée par Fanjita (www.fanjita.org), il s'agit du E-loader 0.97 qui permet aux possesseurs de psp v 2.01 de lancer des homebrews. Bien sur, Sony corrigera la faille et sortira une version du jeu sans la faille ? Certains sites expliquent que selon le numéro que l'on peut lire sur la pochette du jeu, on sait si on a le GTA avec faille ou non. Mais hélas, ce n'est pas une vérité à 100 %, pour en être sur il faut insérer l'UMD de GTA dans la PSP, si vous voyez qu'il propose la mise à jour en 2.0 BINGO vous avez la bonne version, sinon c'est mort pour vous…
Si votre PSP est en 2.01, passez là en 2.5 ou 2.6 (certains disent que c'est mieux de passer en 2.6, personnellement je passe en 2.5 à l'aide d'un UMD et ça ne pose pas de problèmes)
Le pack de Dark Alex est divisé en deux, selon si vous avez une 2.5 ou une 2.6, faites votre choix et copiez le contenue du dossier / DOWNDATERTEST/ dans le le dossier /PSP/GAME/ de votre Memory Stick, puis le dossier / DOWNDATER/ à la racine de la carte mémoire et enfin l'E-loader 0.9.7 de Fanjita.

Vous devriez avoir les dossiers suivant :
• /UTILS/ dans lequel il y a 2 fichiers (EBOOT_signature et touch)
• /PSP/eloader/ dans lequel il y a les 7 fichiers de l'Eboot)

Assurez-vous que votre PSP soit rechargée au maximum et branchez là sur le secteur pour plus de sécurité.
Vous êtes prêt ? Alors lancez le jeu GTA [voir photo downgrader-25-26-14.jpg] (vous pouvez passer les scènes cinématographique pour gagner du temps) et vous allez voir l'E-menu de Fanjita (très rapide), puis le Emenu du Downdate Test [voir photo downgrader-25-26-16.jpg] sur lequel il faudra cliquer pour le lancer, ce qui fera booter sur E-loader…[voir photo downgrader-25-26-17.jpg]
L'écran de la PSP va s'éteindre, si vous observez le voyant du Memory Stick vous verrez que c'est en train d'écrire dessus, ce qui veut dire que le flashage est en cours. Au bout de moins d'une minute la console devrait redémarrer toute seule (si il ne se passait rien, alors éteignez la et rallumez là, mais soyez patient avant d'éteindre la PSP !).
Au redémarrage, vous découvrirez le même message d'erreur que pour le Downgrade 2.0, puis il faudra redéfinir les paramètres de la PSP (la langue, la date, etc.)
Bravo, votre PSP est en 1.5 !

Si ça ne fonctionne pas, regardez à nouveau le tuto et posez vos questions sur www.xavboxforum.com

c) Je suis en 1.5 mais je ne peux plus lancer certains jeux

Une fois repassé avec le firmware 1.5, vous n'aurez plus le navigateur Internet et ne pourrez plus lancer certains jeux qui vous demanderont de mettre à jour votre PSP ?
Bien sur vous n'allez pas remettre à jour à chaque fois puis refaire un downgrader !
Il y a toujours une solution, et la meilleur de toutes s'appel Devhook 0.46 (lorsque vous lirez cet article il y aura peut-être une version plus récente).
Les dernières versions de Devhook (très actif ces temps-ci, sortant plusieurs mises à jour régulièrement) permettent de lancer tout les softs !
Il permet d'émuler (simuler) les firmwares 1.5 à 2.7 et donc offre la possibilité de lancer tout les jeux les plus récents, comme les anciens !
Mais ce n'est pas tout, il permet également de pouvoir utiliser la navigateur Internet qui disparaît dès que l'ont passe en version 1.5.
Le seul soucis, c'est que le paramétrage de ce soft est assez délicat car un mauvais choix dans l'une des options et aucun jeux ne se lance !
Pour faciliter son utilisation, un français nommé Guillou à traduit le soft, mais ça reste quand même difficile à paramétrer si vous n'avez pas de notice… ça fera peut-être l'objet d'un prochain article dans Net Secret's
Pour la PSP, restez informé des mises à jour des softs et découvrez les tutos plus complet sur www.xavboxpsp.com
Et n'oubliez pas que vous devez posséder les originaux des jeux que vous copiez.

Article réalisé par Xavier, webmaster de www.xavbox.info
Photos de Xavbox et Pedro93

Les 7e Rencontres Mond

Comme tous les ans à la même période se tenaient, du 4 au 8 Juillet dernier, les Rencontres Mondiales du Logiciel Libre. NetHacker été bien sûr présent à ce rendez-vous où l'on parle du Libre mais aussi, de la sécurité.

Les Reumeuleuleu

Les Reumeuleuleu, ce sont les Rencontres Mondiales du Logiciel Libre, pour les habitués. Cette année, l'évènement était gracieusement hébergé par la faculté des sciences Henri POINCARÉ de VANDOEUVRE-LEZ-NANCY. Durant 4 jours, 200 conférences, 25 exposants et une dizaine d'ateliers ont accueillis, pour des présentations et des démonstrations, plus de 1500 visiteurs.
Chaque année, c'est l'occasion pour toutes ces personnes de partager leur engouement pour le Libre, et de rencontrer les acteurs qui se cachent derrière tant de projets. Voire parfois même de découvrir certains de ces projets.



L'affiche des RMLL

Les exposants

En entrant dans la pièce principale, toute en longueur, vous découvrez un pare-terre d'exposants : du LUG (Linux User Group) à Mandriva, en passant par OpenOffice et OpenBSD, sans oublier bien sûr la FSF, chacun y trouve son bonheur. Les plus aguicheurs ?

Parmi les stands qui auront attiré les plus de badauds, on comptera certainement deux stands accolés près des portes principales. Deux projets, deux hommes, un même thème : la cartographie GPS (et GPL !). Ils sont a la fois compagnons et concurrents, heureux compères à discuter de leurs travaux. L'un se lance à l'assaut des routes, une boite un peu spéciale sous le siège. L'autre utilise des ordinateurs portables et des récepteurs GPS standards. Et chacun transforme les données brutes reçue pendant leurs vadrouilles pour en faire des cartes dignes des plus grandes cartes. Qui sont-ils? Le premier projet se nomme OpenStreetMap.org, l'autre Un Point C'est Tout (http://upct.org). Quand le premier embarque un ordinateur dans une boite de dérivation, le second s'attache aux corrélations, ces point touristiques et autres curiosités qui bordent les routes et qui méritent leur place sur une carte. Et les contributions sont nombreuses : chaque personne désireuse de « mapper » sa région peut apporter son aide. Un angle ludique est même ouvert par UPCT, qui propose aux écoles de faire découvrir leur ville aux jeunes élèves : cartographie, prise de photo, histoire de la ville et de son patrimoine, tout un programme !

Un peu plus loin, Mandriva fait face à la fondation Mozilla. Deux monstres du Libre venu exposer leurs lignes directrices futures. Et Mandriva était venu en masse : pas moins de 19 représentants étaient sur place. Il faut dire que le distributeur français, récemment détenteur de Connectiva, profitait de l'occasion pour permettre aux équipes Brésilienne et Française de se rencontrer pour la première fois. Nous avons pu demander à toutes ces personnes quel était l'avenir de Mandriva. La réponse la suivante : « Mandriva 2007, qui devrait sortir courant septembre, intégrera de nombreuses nouveauté. La plus importante se situant au niveau de RPMDrake, le gestionnaire de paquet, complètement remodelé. Bien sûr, la mise a jour vers les versions récentes des grosses entités est prévue : KDE3.5, GCC4, ... ». Côté Mozilla, nous engageons avec deux représentants une longue et très intéressante joute verbale sur la cohabitation « gestionnaires de paquets vs. Mise a jour intégrée de Firefox », qui aurait pu porter comme sous-titre « Comment prévenir APT et autres Emerge que Firefox est assez grand pour migrer seul vers une version plus aboutie ». Au final, des idées nombreuses et originales, qui feront peut-être leur chemin (la suite, plus tard, dans NetHacker ;).

Conférences

Dans les amphithéâtres pleins, des têtes habituelles. Cinq jours, ça laisse le temps de repérer des visages. Et

iales du Logiciel Libre


L'ordinateur embarqué de OpenStreetMap.org

de savoir qui posera ou non une question intéressante.
Parce qu'intéressantes, les conférences le sont. Comme sur les stands, les systèmes embarqués sont au goût du jour. Serait-ce l'avenir du Libre? « A l'avenir, Linux ne saura plus entrer dans un robot, tant son poids commence à devenir conséquent ». C'est ce que semble penser l'un des auditeurs, présent à la démonstration des étudiants de l'ESIEA venu décrire leur robot, heureux concurrent du concours E=M6, et fier d'être mû par un OS Libre. Les orateurs tiendrons la paroles pendant plus de deux heures, expliquant pourquoi leur choix s'est tourné vers Linux, et non vers le concurrent direct, Microsoft Windows CE. Un choix qui, contrairement à ce qu'en pense le fameux auditeur, est de plus en plus fait : même si aucun chiffre n'existe, on raconte que 75% des robots du concours comptent leur puissance non pas en chevaux mais en... gnous !
Vient ensuite le tour la virtualisation. Un représentant XEN, apparemment peu expérimenté dans les démonstrations orales, nous propose de découvrir XEN, superviseur de machines virtuelles bien connu. L'idée été bonne, la réalisation un peu moins : entre défilement de fichiers de configuration et vidéos qui ne passent pas sur le vidéoprojecteur (fallait pas inviter Windows Media Player aux RMLL), la démonstration fut courte. Mais qu'importe, quand on connaît son sujet, l'attirail technique n'est qu'un outil : face aux question, le conférencier rattrape largement la donne et réussi à intéresser les curieux.
Ensuite, Jabber. Jabber, vous connaissez certainement, c'est LE protocole d'Instant Messaging en vogue. Avec une architecture décentralisée et une stabilité à toute épreuve, la bête à fait sa réputation. Mais, nous allons, au moment du jeu des questions-réponses, mettre l'accent sur un point faible : la sécurité, et notamment au travers du supports de passerelle MSN/AIM/Yahoo, qui permettent à un utilisateur Jabber de discuter avec ses buddies sur ces trois protocoles, sans utiliser un autre logiciel (ni même un autre compte). Réponse nous sera faite que le support futur de ces passerelles ne sera certainement plus assuré. Concernant la sécurité propre de Jabber, des recherches et un développement sont effectués pour améliorer l'état actuel, déjà bien avancé, avec un support de PGP/GPG ainsi qu'une communication via SSL avec les serveurs. A surveiller.
On vous garde la meilleure « conférence » pour la fin. Conférence, pas vraiment. Il s'agit en fait d'une table ronde politique. Un rendez-vous unique où vous trouvez, de gauche à droite, sur une même table, et sans armes : Christophe ESPERN (fondateur EUCD.INFO), Michel ROCARD (Député Européen, Parti Socialiste), Richard CAZENAVE (Député Assemblée Nationale, Union pour un Mouvement Populaire), Martine BILLARD (Députée de Paris, les Verts) et François BAYROU (Député Assemblée Nationale, Union pour la Démocratie Française). Le tout orchestré par Gilles PELLEGRINI, maître de conférence à l'Ecole Nationale Supérieur d'Electronique, Informatique et Radiocommunications de Bordeaux, dans un amphithéâtre comble. L'ordre du jour de cette table ronde est un débat autour de la loi DADVSI, qui venait alors a


Un amphithéâtre plein pour la table ronde politique

(faut pas avoir faim), tourisme dans Nancy, et rencontres chez l'habitant. Mais l'esprit communautaire, c'est aussi à table qu'on le partage, grâce au repas du Libre : dans un cadre somptueux, autour d'un repas qu'il l'est tout autant (sauté de manchot avec ses petits en sauces ... :D), les discutions sont très riches et les sourires s'affichent nombreux sur les visages. Et si votre ventre n'est pas au centre de toute votre attention, et que les idéaux vous poursuivent même après la clôture d'une journée de RMLL, vous pouvez suivre tout le monde, direction la place de Nancy, et la FNAC, où une grande manifestation anti-DADVSI est organisée. De quoi faire pâlir les gardes de sécurité. Mais tout le monde sait bien que le manchot, même en réunion, est un animal paisible. De toute façon, on sait qui est qui, grâce à la Finger Print Party, qui a eu lieu quelques minutes avant : chacun signe la clef PGP/GPG du voisin, créant un cercle de confiance basé sur l'entrevue physique et la présentation d'une pièce d'identité officielle (on ne transige pas avec les questions de sécurité).

peine d'être adoptée. Un sujet encore houleux sur lequel les discutions ont eu bon train pendant plus de deux heures et demi, dans une atmosphère très détendue par messieurs Michel ROCARD et François BAYROU, qui pimentent le débat de nombreuses répliques humoristique quant à leur appartenance politique respective. La séance est levée. Le public aussi : dix bonne minute de standing ovation, pour les politiques et l'organisateur de la table ronde. Nous sortons de la salle, avec des réponses à nos questions, avec des propositions des ce quintuor à qui nous avons demandé d'agir prestement pour que DADVSI ne soit pas appliquée. Et avec une route en tête : celle qui nous mène vers une salle où se trouve le fameux verre de l'amitié.

Les annexes

Et, que fait-t-on quand on a visité les stands 17 fois, interviewé une personne par stand, assisté aux conférences qui correspondent le plus à notre profil? Ils pensent donc à tous, ces GO. Au sous-sol, c'est un peu la règle du « Quand il n'y en a plu, il y en a encore ». Place aux ateliers : seul ou entres amis, face à un ordinateur, quelqu'un de compétent vous fait découvrir ces choses magnifiques qu'on peut réussir avec le libre. Et il faut plus de temps pour le décrire que pour le faire, puisqu'accompagnés par ces experts, vous tapez en quelques minutes un texte aussi bien mis en page que ne l'aurait fait un imprimeur, grâce à LaTeX; l'âme du graphiste naît en vous quand en seulement quelques dizaines de ces même minutes, un manchot jailli de votre écran : vous maîtrisez (presque) Blender. Et la liste est longue, puisque ces ateliers étaient des itinérants de l'horloge, des éphémères ne durant au plus qu'une journée sur la calendrier des RMLL...

Et après? Quand on a fait tout ça? Question simple, réponse simple : la journée est terminée, on va penser à manger. Ça aurait pu être « met un rosé, Jean-Jacques », ce sera plutôt « Met un demi, Robert ». Des activité annexes sont aussi prévues par les GO (ils sont bons, ils sont bons) : visite de Brasserie

CONCLUSION

5 jours, c'est très court. Il faut rencontrer tous les chefs de projets présents, discuter avec eux des évolutions, depuis nos dernières rencontres. Il faut découvrir ces projets qui restent inconnus mais qui sont promis à un bel avenir. Les RMLL, c'est exactement cela : les Rencontres Mondiales. On y rencontre, on y découvre, et on y retourne l'année d'après.

Snake & Koreth

COURRIER DES LECTEURS

Bonjour,

Félicitations pour votre magazine, il gagne en maturité de numéro en numéro. Après deux premiers numéros assez mauvais, j'ai quand même acheté le 3è qui est totalement différent. Ensuite le 4è meilleur que le précédent. Vivement le 5è ...

Ce magazine me permet de mieux comprendre les « secrets des hackers ». Pensez-vous aborder en détails les protocoles ? Aborderez-vous le wifi ?

Merci à FaSm pour ses articles très didactiques sur l'assembleur qui m'ont permis de m'y mettre malgré mes réticences.

Merci et bonne continuation
Alix

Alix,

Merci pour les compliments. Nous ne reviendrons que peu sur le changement d'équipe, à l'origine du changement profond que connaît actuellement le magazine. Parmi ces changements, nous désirons avant tout donner aux lecteurs satisfactions. Pour ce faire, il est normal que nous écrivions sur ce que nos amis lecteurs désirent lire. Ainsi, nous prenons la demande de papier sur les protocoles et le wifi comme une requête, et nous écrirons prochainement les articles en conséquences. Nous espérons alors avoir de vos nouvelles quand à la qualité de ces futurs articles.

Merci de votre fidélité

Bonjour et bravo pour la qualité de votre magazine.

Je suis intéressé par un double boot XP/Linux, et votre article est très intéressant à ce sujet. Mais moi je possède un disque dur de 160 GO et je n'ai pas d'espace libre C 143Go en NFTS et D 5.98Go en FAT 32, peut on créer de l'espace libre sans réinstaller XP.

Merci de votre réponse
YOYO un fidèle lecteur

Bonjour Yoyo,

Merci, au même titre que pour Alix, pour les gentillesses. Concernant votre problème, il s'agit d'une opération un peu plus pointue qu'un simple partitionnement, mais vous n'êtes pas le seul dans ce cas, et pour cause, nombreuses sont les personnes qui ont eu l'habitude de faire sans Linux et donc d'utiliser à 100% leur disque dur. Libérer de la place en devient des plus difficile.

Une solution pourtant existe. Sous plusieurs logiciels. Le premier, PartitionMagic, est depuis peu un produit Symantec (Norton Antivirus, Ghost, ...). Mais, comme tout logiciel propriétaire, PartitionMagic connaît des équivalents libre, comme l'excellent Gparted, qui lui ressemble comme deux goûtes d'eaux. On connaît aussi un certain qtParted, dans ce domaine. Le Net fournira la documentation nécessaire, tant que NetHacker ne saura vous fournir un article sur ce sujet.

sommaire du prochain numéro



News

Programmation :
- Femme de geeks : la vie au quotidien
- Un client / serveur facile

Sécurité :
- Les trojans , kesako ?
- Vos traces sur internet

Crakers :
- Reverse ton MSN
- Crackme de la ndh

Reseau :
- Le wifi chez soi

Dossier :
- Le wardriving

Windows :
- Les commandes dos
- Les scripts existent aussi sous windows

Linux :
- Partagez vos fichiers sous linux avec NFS

Web :
- C'est quoi une css

Gamers :
- Les nouveautés consoles

Culture :
- Comment fait on pour devenir informaticien ?

Courrier des lecteurs

Courrier des lecteurs
netsecrets@acissi.net

irc.worldnet.net channel : #netsecrets

Forum : acissi.net/forum

AC'ISSI

Retrouvez nous sur le site :
acissi.net